# WELL mPBX-U110R

## Administrator's Guide

Version 12.17.0.30

# Table of Contents

1. Introduction ..... 5
1.1 Features ..... 6
1.2 Hardware Specifications ..... 7
1.2.1 Exterior Appearance ..... 7
2. System setup ..... 8
2.1 Connection Drawing ..... 8
2.2 Connecting Ethernet Line ..... 8
2.3 Supplying Power ..... 8
3 Administrator Login ..... 9
4 Status ..... 10
4.1 Line status ..... 10
4.1.1 Extension Status ..... 10
4.1.2 Trunk Status ..... 11
4.2 System Status ..... 12
4.2.1 System Info ..... 12
4.2.2 Network Status ..... 12
5 System ..... 13
5.1 Network Preferences ..... 13
5.1.1 LAN Settings ..... 13
5.1.2 WAN Settings ..... 15
5.1.3 DHCP Server ..... 16
5.1.4 VLAN Settings ..... 17
5.1.5 VPN Settings ..... 19
5.1.6 DDNS Settings ..... 19
5.1.7 Static Route ..... 20
5.2 Firewall Settings ..... 21
5.2.1 Firewall Rules ..... 22
5.2.2 IP blacklist ..... 24
5.3 System Preference ..... 25
5.3.1 Password Settings ..... 25
5.3.2 Date and Time ..... 25
5.3.3 Firmware Update ..... 26
5.3.4 Hot Standby ..... 27
5.3.5 Backup and Restore ..... 29
5.3.6 Reset and Reboot ..... 29
5.3.7 Alert Settings ..... 30
5.3.8 Addons ..... 32
5.4 Storage Management ..... 33
5.4.1 External Storage ..... 33
6 PBX ..... 36
6.1 Extensions ..... 36
6.1.1 FXS/VoIP Extensions ..... 36

FXS Extensions ..... 36
VoIP Extensions ..... 41
6.1.2 Phone Provisioning ..... 46
6.2 Trunks ..... 54
6.2.1 Physical Trunk ..... 55
6.2.2 VoIP Trunk ..... 58
6.3 Outbound Call Control ..... 64
6.3.1 Outbound Routes ..... 64
6.3.2Speed Dial Settings ..... 66
6.4 Inbound Call Control ..... 67
6.4.1 IVR ..... 67
6.4.2 Ring Groups ..... 69
6.4.3 Queues ..... 71
6.4.4 Conferences ..... 75
6.4.5 Inbound Routes ..... 75
6.5 Audio Settings ..... 80
6.5.1 Custom Prompts ..... 80
6.5.2 Music on Hold Prompts ..... 81
6.5.3 System Prompts Settings ..... 82
6.6 Basic Settings ..... 82
6.6.1 General Preferences ..... 83
6.6.2 Business Hours ..... 85
6.6.3 Feature Codes ..... 86
6.6.4 Voicemail Settings ..... 89
6.7 Advanced Settings ..... 92
6.7.1 SIP Settings ..... 92
6.7.2 IAX Settings ..... 98
6.7.3 Blacklist ..... 99
6.7.4 Callback Settings ..... 100
6.7.5 DNIS Settings ..... 101
6.7.6 DISA ..... 102
6.7.5 PIN User Settings ..... 103
6.7.8 Paging Groups ..... 105
7 Reports ..... 107
7.1 Call Logs ..... 107
7.2 System Logs ..... 107
8 Logout ..... 108
9. Use mPBX ..... 109
9.1 Make outbound call ..... 109
9.1.1 Sample Routing via E1 Trunk ..... 109
9.1.2 Sample Routing via VoIP Trunk ..... 110
9.2 Incoming call ..... 112
9.2.1 Sample Routing to an IVR ..... 112

APPENDIX A FAQ ..... 115
APPENDIX B How to Configure Autobackup ..... 116
APPENDIX C How to Configure NAT setting ..... 118
APPENDIX D How to Use Auto Provision ..... 120
APPENDIX E HowDo I Configure Distinctive Ring Tones ..... 123
APPENDIX F How to Use DID ..... 125
APPENDIX G mPBX Security configuration Guide ..... 129
1. Security Configuration for Web GUI ..... 129
1.1 Change the default access port for HTTP on Options page ..... 129
1.2 Change the default password for the web GUI ..... 130
2. Disable SSH on LAN Settings Page ..... 130
2.1 Disable SSH ..... 130
2.2 Change the default password for SSH ..... 131
3. Security Configuration for Extensions ..... 132
3.1 Change the default SIP Port ..... 132
3.2*Disable guest calls ..... 133
3.3* Security Configuration for remote extensions ..... 133
3.4 Set an enhanced password and enable IP restriction for extensions ..... 134
4. Setup Proper Firewall Rules ..... 135
5*. Alert Settings ..... 142
5.1 IPATTACK ..... 143
5.2 WEBLOGIN ..... 144
6. Note ..... 145

# 1. Introduction

## mPBX —IP-PBX for Medium Businesses/Home Office

WELL mPBX-U110R is a standalone embedded hybrid PBX for medium businesses and remote branch offices of larger organizations (1-100 users per site). WELL mPBX-U110R also offers a hybrid solution (a combination of VoIP applications using E1/T1/J1 equipment) alternative for enterprises who are not yet ready to migrate to a complete VoIP solution.

**FCC Statement**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radiofrequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

**FCC Caution**

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

**FCC Warning**

This equipment has been tested and found to comply with the regulations for a Class B digital device, pursuant to Part 15 of the FCC Rules.
Operation is subject to the following two conditions:
(1) This device may not cause harmful interference.
(2) This device must accept any interference received including interference that may cause undesired operation.

# 1.1 Features

| | |
|---|---|
| • Auto-provision | • Follow me |
| • Audio In/Out | • Interactive Voice Response (IVR) |
| • BLF Support | • Intercom / Zone Intercom |
| • Blacklist | • Music On Hold |
| • Call transfer | • Music On Transfer |
| • Call Detail Records(CDR) | • Paging / Zone Paging |
| • Call Forward | • PIN Users |
| • Call Parking | • Queue |
| • Call Recording | • QOS |
| • Call Pickup | • Ring Group |
| • Call Routing | • Route by Caller ID |
| • Call Transfer | • Spy functions |
| • Call Waiting | • Skype Integration (Skype Connect) |
| • Caller ID | • Three-way Calling |
| • Call Back | • Mobility Extension |
| • Conference | • External Storage |
| • Speed Dial | • DDNS |
| • Define Office Time | • OpenVPN |
| • Direct Inward System Access(DISA) | • T.38 |
| • DIDs | • Voicemail |
| • Distinctive Ringtone | • VLAN |
| • Do Not Disturb(DND) | • WAN |
| • Dial by Name | • PPPoE |
| • Firewalls | • Static Route |
| • Alert | • Multiple administrators |
| • Integrated built-in packet capture tools | • Blind Transfer |

More info, please click: http://www.yeastar.com/Products/mPBX-U300.asp

# 1.2 Hardware Specifications

## 1.2.1 Exterior Appearance

**Front Panel**

Figure1-1 WELL mPBX-U110R Front Panel

| No. | Indication |
|---|---|
| ① | Reset button: Press until all LEDs turn orange, which means the reset is completed. |
| ② | Power LED: Green stably<br>Run LED: Green Blinking |
| ③ | Audio in interface<br>Audio out interface |
| ④ | USB 2.0 port |
| ⑤ | WAN port<br>LAN port |
| ⑥ | Console port (RJ45) |
| ⑦ | E1/T1 interface |
| ⑧⑨ | Two fixed FXS ports(RJ11) |

# 2. System setup

## 2.1 Connection Drawing

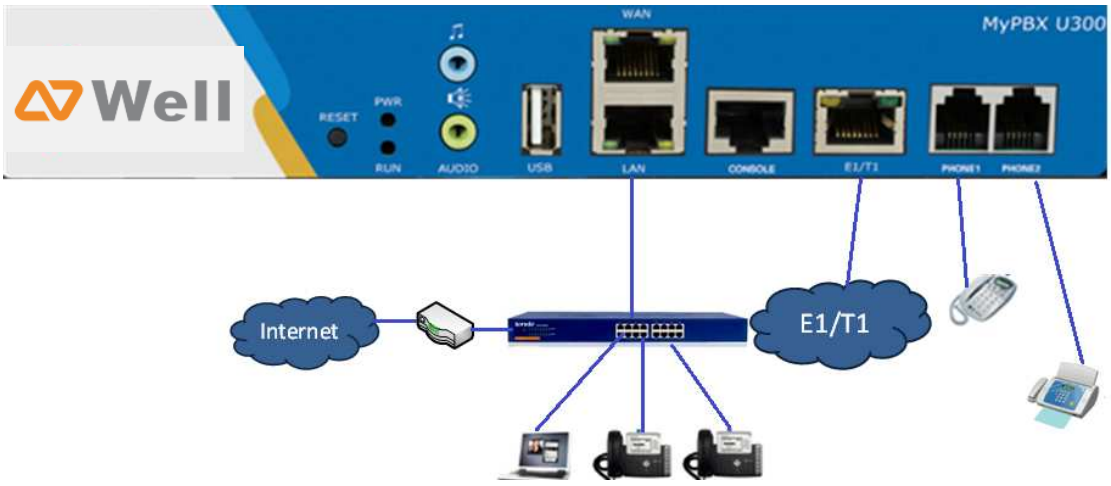



Figure 2-1

## 2.2 Connecting Ethernet Line

mPBX provides two 10/100MEthernet ports with RJ45 interface and LED indicator. Plug Ethernet line into mPBX's Ethernet port, and then connect the other end of the Ethernet line with a hub, switch, router, LAN or WAN. Once connected, check the status of the LED indicator. A yellow LED indicates the port is in the connection process, and a green LED indicates the port is properly connected.

## 2.3 Supplying Power

Please follow the steps below to connect the mPBX unit to a power outlet:

1. Connect the small end of the power cable to the power input port on the mPBX back panel, and plug the other end of the cable into a 100V~240V AC power outlet.
2. Check the Power LED on the front panel. A solid green LED indicates that power is being supplied correctly.

# 3 Administrator Login

From your web browser, input the IP address of the mPBX server.
If this is the first time you are configuring mPBX, please use the default settings below (your PC should be in the same local network with mPBX):
IP Address: http://192.168.5.150
Username: admin
Password: password
In this example, the IP address is 192.168.5.193

Figure 3-1

This is the welcome page of WELL mPBX-U110R after successful login.

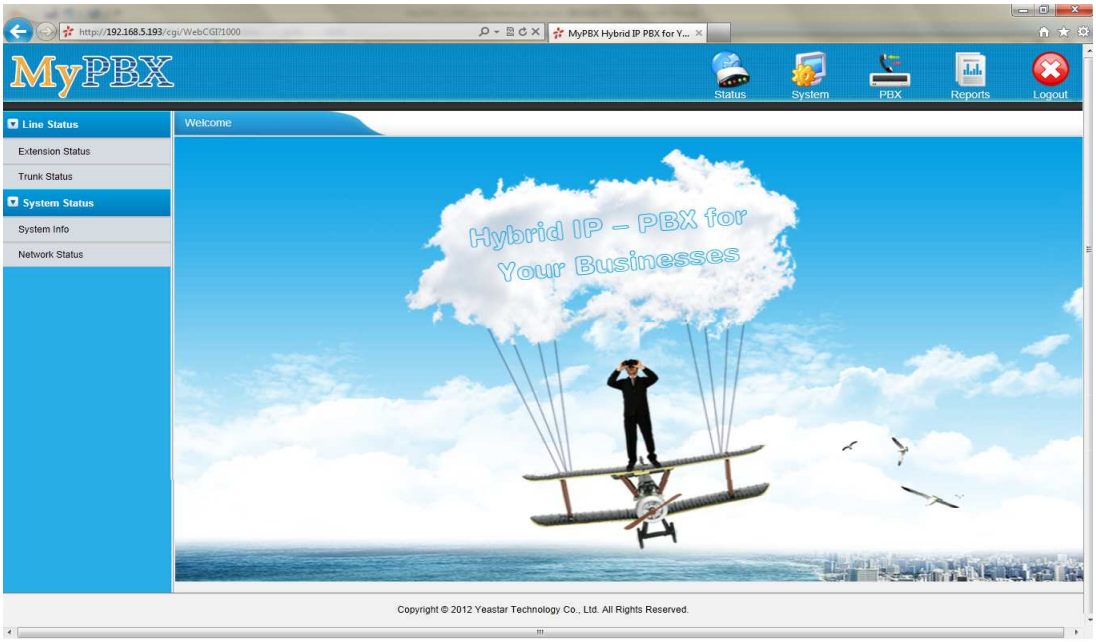



Figure 3-2

# 4 Status

Click

to start to check the status of WELL mPBX-U110R,where we can check the status of extension, trunk, network and system information.

## 4.1 Line status

In this page, we can check the status of extension and trunks

### 4.1.1 Extension Status

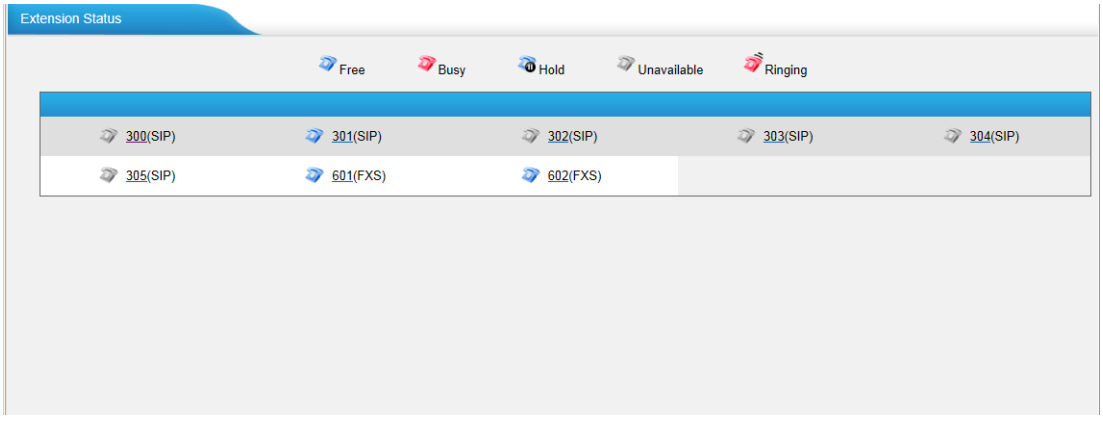


Figure 4-1

**mPBX Status Description:**

**Extensions:**

1) : Extension is unavailable

2) :Extension is idle

3）:Extension is ringing

4）:Extension is busy

5）: Extension is on hold

## 4.1.2 Trunk Status

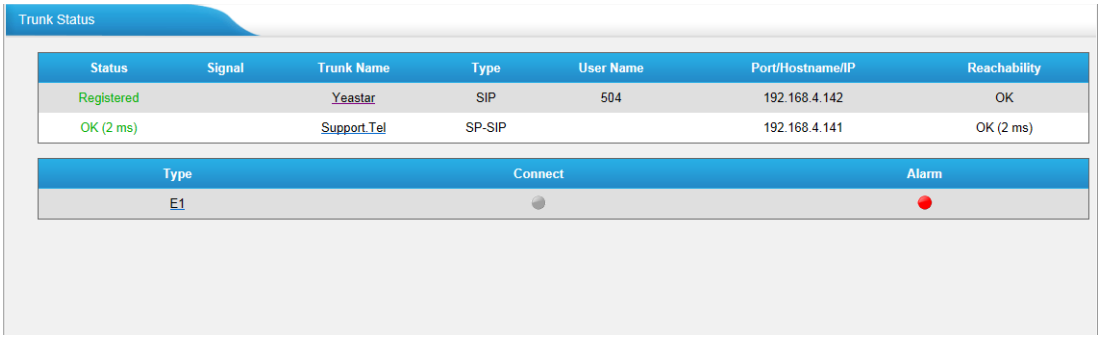



Figure 4-2

**Trunks:**

**VOIP Trunk**:

**Status**

Unregistered: Trunk registration failed.

Registered: Successful registration, trunk is ready for use.

Request Send: Registering.

Waiting: Waiting for authentication.

**Service Provider**:

**Status**

OK: Successful registration, trunk is ready for use.

Unreachable: The trunk is unreachable.

Failed: Trunk registration failed.

**E1 Trunk**:

| Connect | Alarm | Comment |
|---|---|---|
| | | The port doesn't have E1 line connected. |

| | | |
|---|---|---|
| | | E1 line has been connected to the port; PRI is in corresponding or can't communicate. |
| | | Succeed. |

## 4.2 System Status

In this page, we can check the status of mPBX system, including the hardware, firmware version and the network status of LAN and WAN ports .

### 4.2.1 System Info

In this page, we can check the hardware/firmware version, or the disk usage of mPBX.

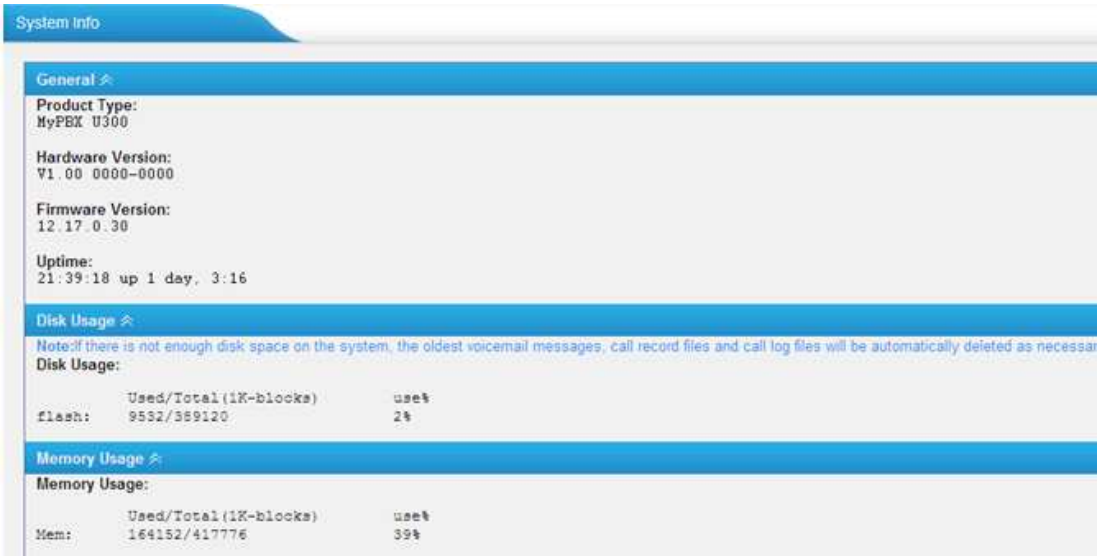



Figure 4-3

### 4.2.2 Network Status

In this page, the IP address of LAN and WAN port will appear, if OpenVPN and Vlan are configured well, they will be display here too.

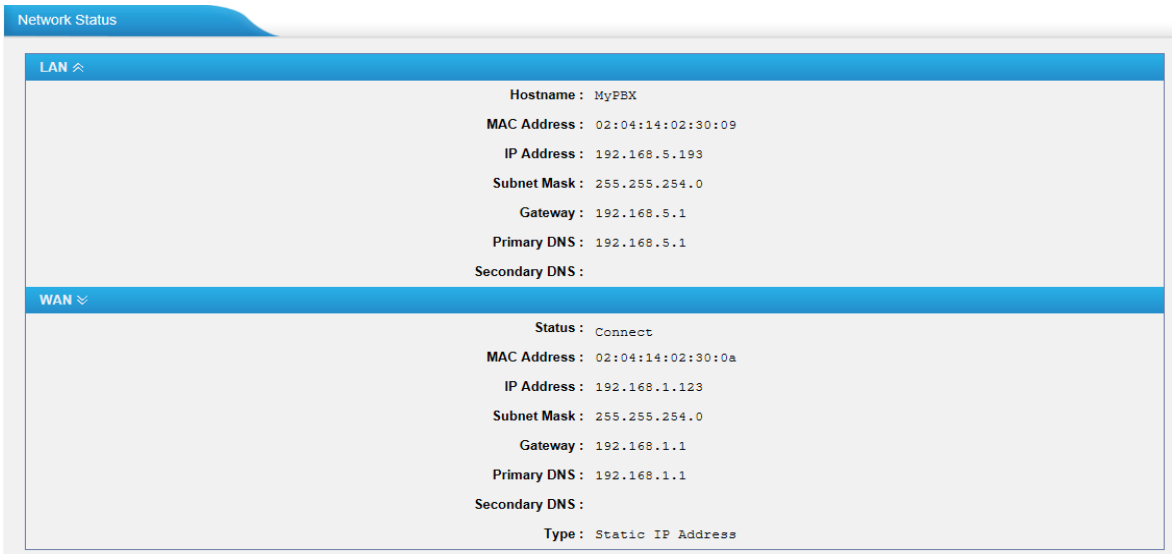



Figure 4-4

# 5 System

Click

to access.

In this page, we can configure the network settings, firewall settings, storage management and some other preferences like firmware update and hot standby.

## 5.1 Network Preferences

### 5.1.1 LAN Settings

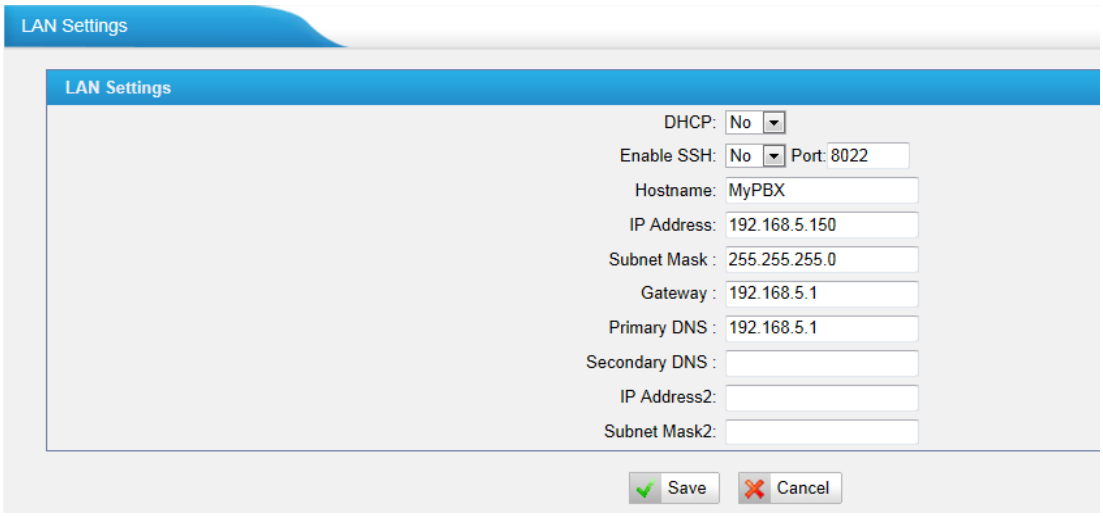



Figure 5-1

**·DHCP**

If this option is set, mPBX will use DHCP to get an available IP address from your local network. Not recommended or you cannot access mPBX without the right IP address

**·Enable SSH**

This is the advance way to access the device, you can use the putty software to access the device.In the SSH access, you can do more advance setting and debug. Disabled by default.

**·Port**: the default is 8022, you change it to another one

**·Hostname**

Set the host name for mPBX.

**·IP Address**

Set the IP Address for mPBX.
Recommend to configure a static IP address for mPBX

**·Subnet Mask**

Set the subnet mask for mPBX.

**·Gateway**

Set the gateway for mPBX.

**·Primary DNS**

Set the primary DNS for mPBX.

**·Secondary DNS**

Set the secondary DNS for mPBX.

**·IP Address2**
Set the second IP Address for mPBX.

**·Subnet Mask2**
Set the second subnet mask for mPBX.

## 5.1.2 WAN Settings

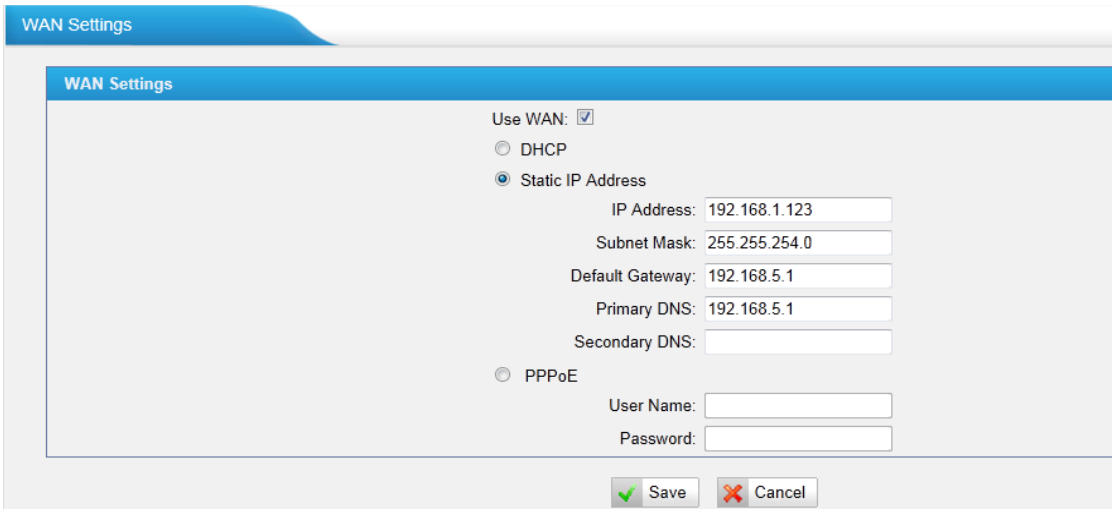



Figure 5-2

It support three connection types: DHCP (obtain an IP automatically), PPPoE, Static IP Address.

**Note:**
1. WAN port is disabled by default
2. WAN port cannot be used as a router to route the internet packages from WAN port to LAN port.

**·DHCP**
.If your ISP says that you are connecting through DHCP or a dynamic IP address from your ISP, perform these steps:
Step1: Select **DHCP** as the WAN Connection Type.
Step2: Click **Save** button to save the settings.
Step3: Reboot the device.
Step4: Check the WAN's Status (Status→ Network status).

**·Static IP Address**
If your ISP says that you are connecting through a static or fixed IP address from your ISP, perform these steps:
Step1: Select **Static IP Address** as the WAN Connection Type.

Step2: Enter the IP Address.
Step3: Enter the Subnet Mask.
Step4: Enter the Gateway Address.
Step5: Enter the Primary DNS and Secondary DNS.
Step6: Click the **Save** button to save the settings.
Step7: Reboot the device.
Step8: Check the WAN's Status (Status→ Network status).

**·PPPoE**

If your DSL provider says that you are connecting through PPPoE or if you normally enter a user name and password to access the Internet, perform these steps:

Step1: Select **PPPoE** as the WAN Connection Type.
Step2: Enter the User Name.
Step3: Enter the Password.
Step4: Click the **Save** button to save the settings.
Step5: Reboot the device.
Step6: Check the WAN's Status (Status→ Network status)

## 5.1.3 DHCP Server

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network. You can set a local network NTP server for mPBX here too

Note: WELL mPBX-U110R can be working as a DHCP server, but cannot be regarded as an router. When using 'Phone Provisioning' for Grandstream IP phone, Enter the IP address of the server directly, e.g.:192.168.5.150; for other phones using the default configuration.

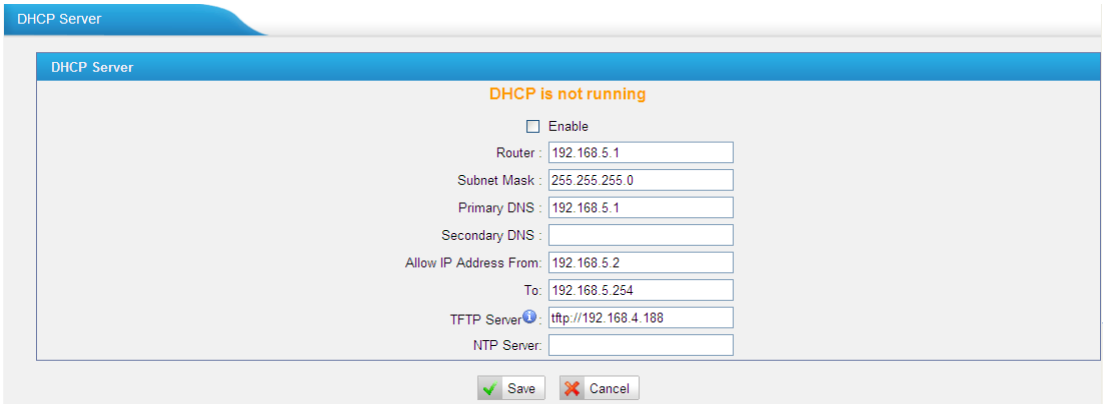



Figure 5-3

## 5.1.4 VLAN Settings

A VLAN(Virtual LAN) is a logical local area network (or LAN) that extends beyond a single traditional LAN to a group of LAN segments, given specific configurations.

**Note:**
WELL mPBX-U110R is not the VLAN server, a 3-layer switch is still needed, please configure the VLAN information there first, then input the details in mPBX, so that the packages via mPBX will be added the VLAN label before sending to that switch.

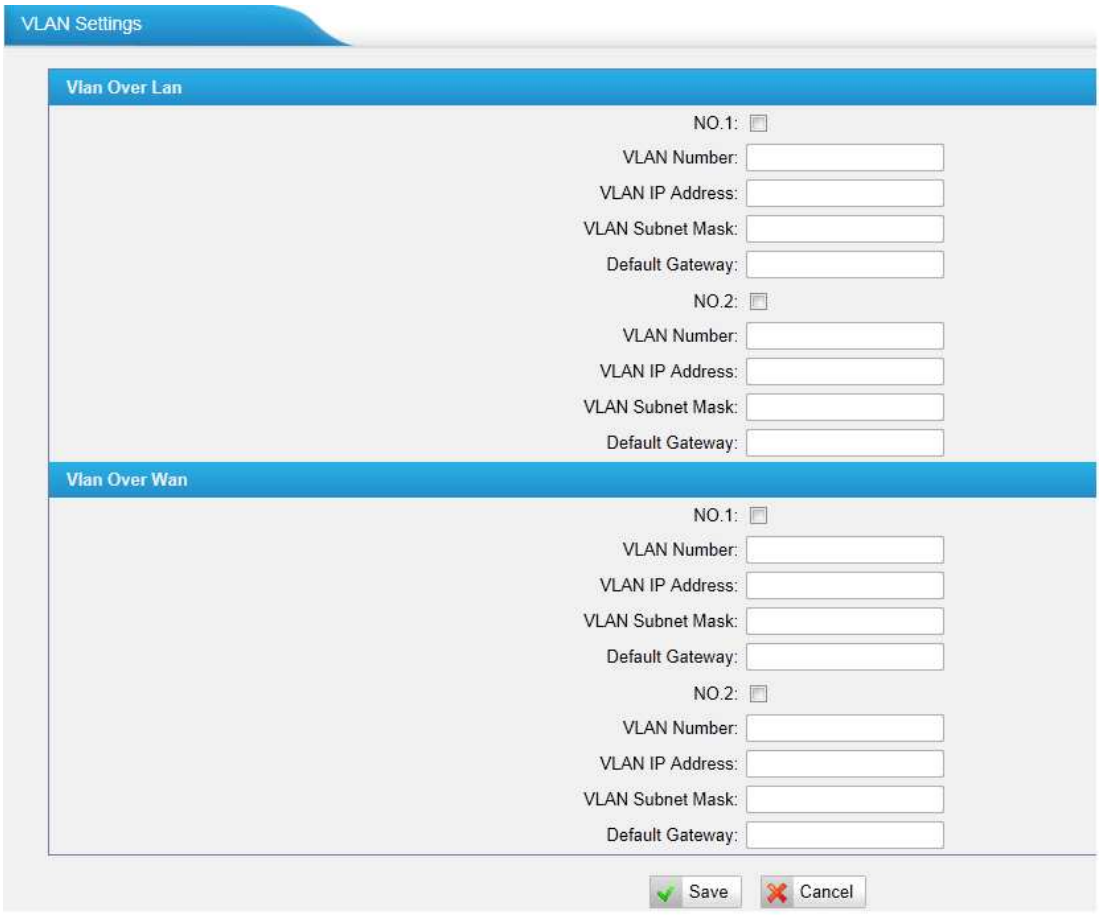



Figure 5-4

1) VLAN Over Lan

**·NO.1**
Click the NO.1 you can edit the first VLAN over Lan.

**·VLAN Number**
.The VLAN Number is a unique value you assign to each VLAN on a single device.

**·VLAN IP Address**

Set the IP Address for mPBX VLAN over Lan.

**·VLAN Subnet Mask**
Set the Subnet Mask for mPBX VLAN over Lan.

**·Default Gateway**
Set the Default Gateway for mPBX VLAN over Lan

**·NO.2**
Click the NO.2 you can edit the first VLAN over Lan.
**·VLAN Number**
.The VLAN Number is a unique value you assign to each VLAN on a single device.

**·VLAN IP Address**
Set the IP Address for mPBX VLAN over Lan.

**·VLAN Subnet Mask**
Set the Subnet Mask for mPBX VLAN over Lan.

**·Default Gateway**
Set the Default Gateway for mPBX VLAN over Lan.

2) VLAN Over Wan

**·NO.1**
Click the NO.1 you can edit the first VLAN over Wan.

**·VLAN Number**
.The VLAN Number is a unique value you assign to each VLAN on a single device.

**·VLAN IP Address**
Set the IP Address for mPBX VLAN over Wan.

**·VLAN Subnet Mask**
Set the Subnet Mask for mPBX VLAN over Wan.

**·Default Gateway**
Set the Default Gateway for mPBX VLAN over Wan.

**·NO.2**
Click the NO.2 you can edit the first VLAN over Wan.

**·VLAN Number**
.The VLAN Number is a unique value you assign to each VLAN on a single device.

**·VLAN IP Address**
Set the IP Address for mPBX VLAN over Wan.

**·VLAN Subnet Mask**
Set the Subnet Mask for mPBX VLAN over Wan.

**·Default Gateway**
Set the Default Gateway for mPBX VLAN over Wan.

## 5.1.5 VPN Settings

A virtual private network (VPN) is a method of computer networking--typically using the public internet--that allows users to privately share information between remote locations, or between a remote location and a business' home network. A VPN can provide secure information transport by authenticating users, and encrypting data to prevent unauthorized persons from reading the information transmitted. The VPN can be used to send any kind of network traffic securely. mPBX supports OpenVPN.

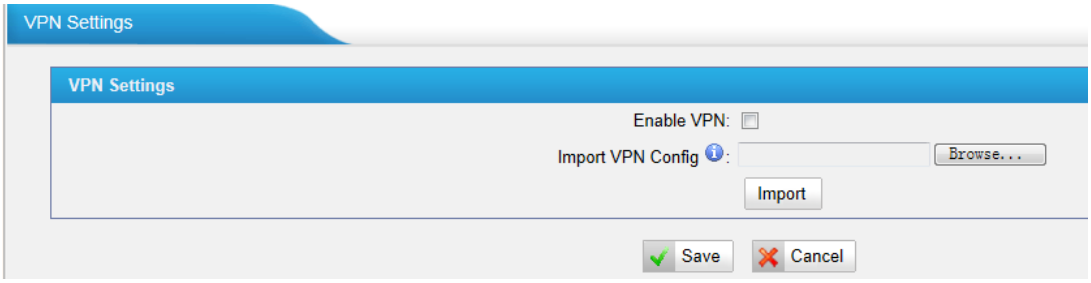



Figure 5-5

**·Enable VPN**

**·Import VPN Config**
Import configuration file of OpenVPN.
Note: Don't configure 'user' and 'group' in the 'config' file.
You can get the config package from the OpenVPN provider.

## 5.1.6 DDNS Settings

DDNS(Dynamic DNS) is a method / protocol / network service that provides the capability for a networked device, such as a router or computer system using the Internet Protocol Suite, to notify a Domain Name System (DNS) name server to change, in real time, the active DNS configuration of its configured hostnames, addresses or other information.

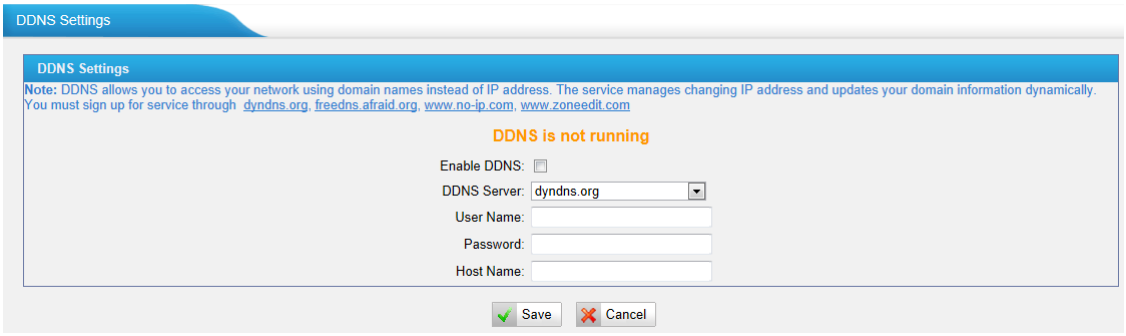

DDNS Settings
DDNS Settings
Note: DDNS allows you to access your network using domain names instead of IP address. The service manages changing IP address and updates your domain information dynamically.
You must sign up for service through dyndns.org, freedns.afraid.org, www.no-ip.com, www.zoneedit.com
DDNS is not running
Enable DDNS:
DDNS Server: dyndns.org
User Name:
Password:
Host Name:
Save
Cancel

Figure 5-6

**·Enable DDNS**

**·DDNS Server**

Select the DDNS server you sign up for service.

**·User Name**

User name the DDNS server provides you. This field is allowed to input 63 characters.

**·Password**

User account's password .

**·Host Name**

**Note**: DDNS allows you to access your network using domain names instead of IP address. The service manages changing IP address and updates your domain information dynamically. You must sign up for service through dyndns.org, freedns.afraid.org, www.no-ip.com, www.zoneedit.com

## 5.1.7 Static Route

mPBX will have more than one internet connection in some situations but it has only one default gateway. You will need to set some Static Route for mPBX to force it goes out through different gateway when access to different internet.
The default gateway priority of mPBX from high to low is OpenVPN→WAN port→LAN port.

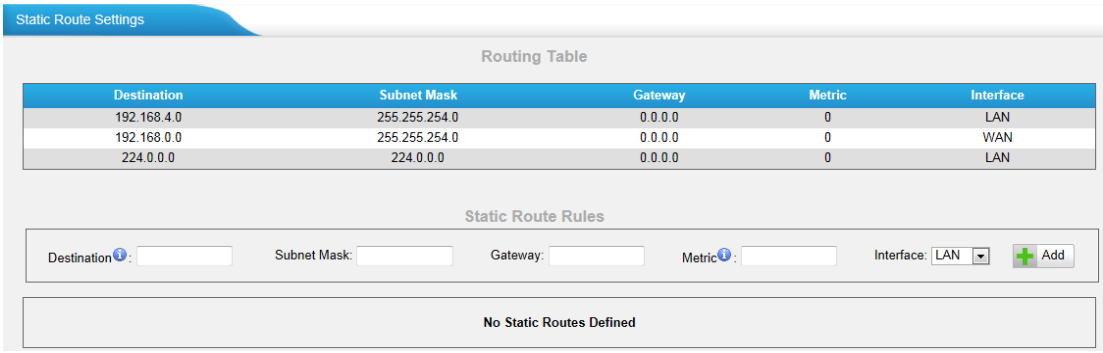



Figure 5-7

1) Route table

The current route rules of mPBX

**·Destination**

The destination network to be accessed to by mPBX

**·Subnet Mask**

Specify the destination network portion.

**·Gateway**

Define which gateway mPBX will go through when access to the destination network.

**·Metric**

The cost of a route is calculated by using what are called routing metric. Routing metrics are assigned to routes by routing protocols to provide measurable statistic which can be used to judge how useful (how low cost) a route is.

**·Interface**

Define which internet port to go through.

2) Static Route Rules

You can add new static route rules here.

# 5.2 Firewall Settings

Firewalls are used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

## 5.2.1 Firewall Rules

Figure 5-8

1) General Settings

**·Enable Firewall**

Enable the firewall to protect the device. You should reboot the device to make the firewall run successfully.

**·Disable Ping**

Enable this item, net ping from remote hosts will be dropped.

**·Drop All**

When you enable 'Drop All' feature, system will drop all packets or connection from other hosts if there are no other rules defined. To avoid locking the devices, at least one 'TCP' accept common rule must be created for port used for SSH access, port used for HTTP access and port sued for CGI access.

2) Common Rules

There is not default rules inside, you can create them as required

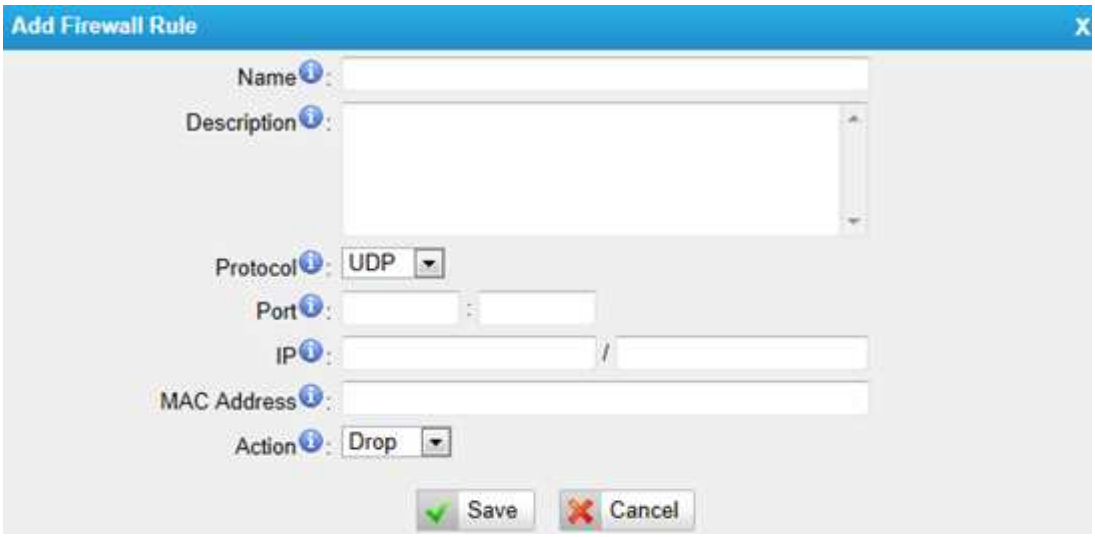



Figure 5-9

**·Name**

A name for this rule, e.g. 'HTTP'.

**·Description**

Simple description for this rule. E.g.: Accept the specific host to access the web interface for configuration.

**·Protocol**

The protocols for this rule.

**·Port**

Initial port should be on the left and end port should be on the right.
The end port must be equal to or greater than start port.

**·IP**

The IP address for this rule. The format of IP address is: IP/mask
Ex:192.168.5.100/255.255.255.255forIP 192.168.5.100
Ex:216.207.245.47/255.255.255.255 for IP 216.207.245.47
Ex:192.168.5.0/255.255.255.0 for IP from 192.168.5.0 to 192.168.5.255 .

**·MAC Address**

The format of MAC Address is XX:XX:XX:XX:XX:XX, X means 0~9 or A~F in hex, the A~F are not case sensitive.

**Note**: The MAC address will be changed when it's remotely device, so it will not be working to filter using MAC for remote devices.

**·Action**

Accept: Accept the access from remote hosts.
Drop: Drop the access from remote hosts.

Ignore: Ignore the access.

## 5.2.2 IP blacklist

You can set some packets accept speed rules here. When a IP address which hasn't been accepted in common rules sends packets faster than the allowed speed, it will be set as black IP address and blocked automatically.

Figure 5-10

1) Blacklist rules

We can add the rules for IP blacklist rate as your demand

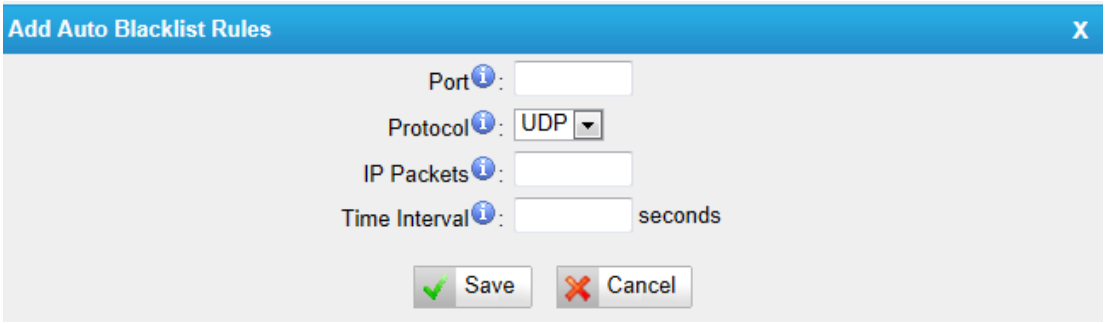



Figure 5-11

**·Port**

Auto defense port

**·Protocol**

Auto defense protocol. TCP or UDP.

**·IP Packets**

Allowed IP packets number in the specific time interval.

**·Time interval**

The time interval to receive IP packets. For example, IP packets 90,time interval 60 means 90 IP packets are allowed in 60 seconds.

2) IP blacklist

The blocked IP address will display here, you can edit or delete it as your wish.

# 5.3 System Preference

In this page, we can set other system preference, like the password for admin account, system date and time, firmware update, hot standby, backup and restore, reset and reboot.

## 5.3.1 Password Settings

1) Change Password

**●User**
mPBX support 3 levels users, choose one of them to change its password.
Administrator: have all authority
User Administrator: have basic authority; without the advanced authority to reset, update, backup and restore mPBX.
CDR Administrator: only have the authority to check the call recordings.

**●Enter Old Password**
The default password of all users is '**password**'.

**●Enter New Password**

**●Retype New Password**
To change the password, enter the new password and click update. The system will then prompt you re-login using your new password.

2) CDR settings
Whether enable CDR User.
Note: To logon mPBX with CDR Administrator, enable CDR user first.

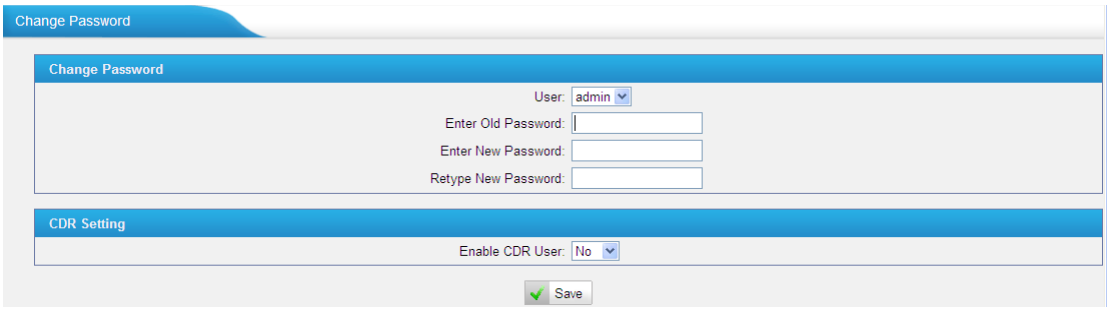



Figure 5-12

## 5.3.2 Date and Time

Set the date and time for mPBX.

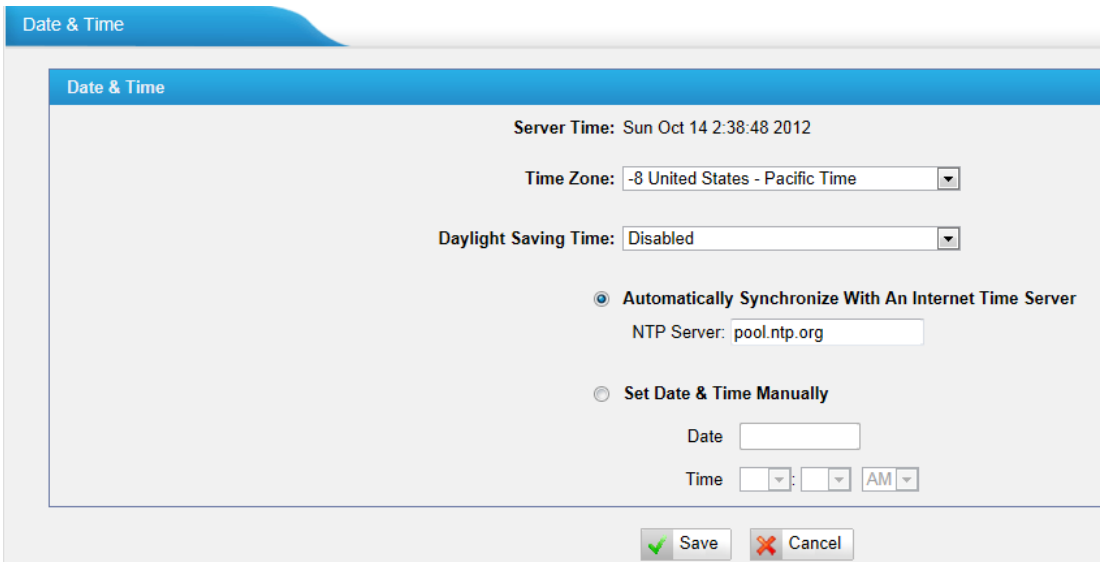



Figure 5-13

**·Time Zone**

You can choose your time zone here.

**·Daylight Saving Time**

Set the mode to Automatic or disabled

**·Automatically Synchronize With an Internet Time Server**

Input the NTP server so that mPBX will update the time automatically

**·Set Date & Time Manually**

You can set the time to your local right time manually here

## 5.3.3 Firmware Update

Upgrading of the firmware is possible through the Administrator web interface using a TFTP Server or an HTTP URL.

Enter your TFTP Server IP address and firmware file location, then click start to update the firmware

**Note:**

1. If enabled 'Reset configuration to Factory Defaults', System will restore to factory default settings.
2. When update the firmware, please don't turn off the power. Or the system will get damaged.
3. More information for the steps to update the firmware, please refer to this link: http://www.yeastar.com/download/mPBX_U300_FirmwareUpgrade_en.pdf

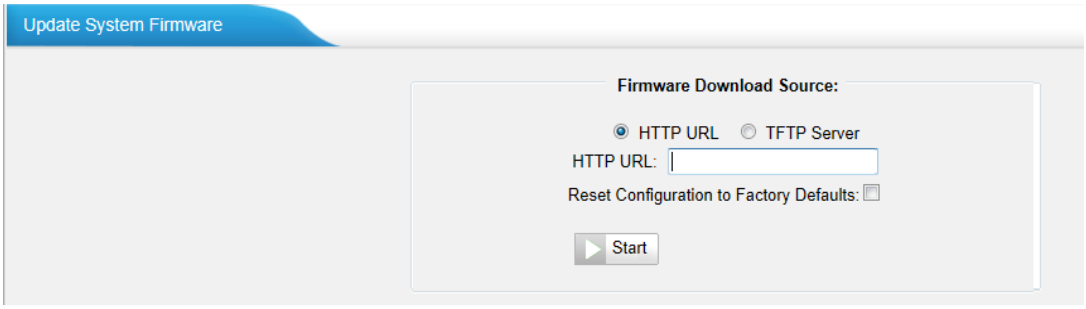



Figure 5-14

## 5.3.4 Hot Standby

Redundancy is achieved by using duplicate hardware and software installations and synchronizing data and operating state. Redundancy assures smooth operation even if a system goes down. Essentially a duplicate backup system takes over with virtual no loss of service. This technique assures absolute reliability no matter what failure occurs. In mission critical installations, redundancy is a way to address possibility of any failure.

**Note 1:** Before enabling the Host Standby feature, please make sure that the two servers in the failover pair are the same model, have the same modules installed in the same slots, the same hardware configurations and firmware version.

**Note 2**: Please configure the primary server first and configure the secondary server only after the running status of primary server becomes "active".

**Note 3:** The virtual IP address inputted in this page will be the one used for registering in each IP phone.

**Note 4**: Before configure the Email list in this page, please configure the 'voicemail settings' in "PBX→Basic settings", make sure the SMTP testing successfully.

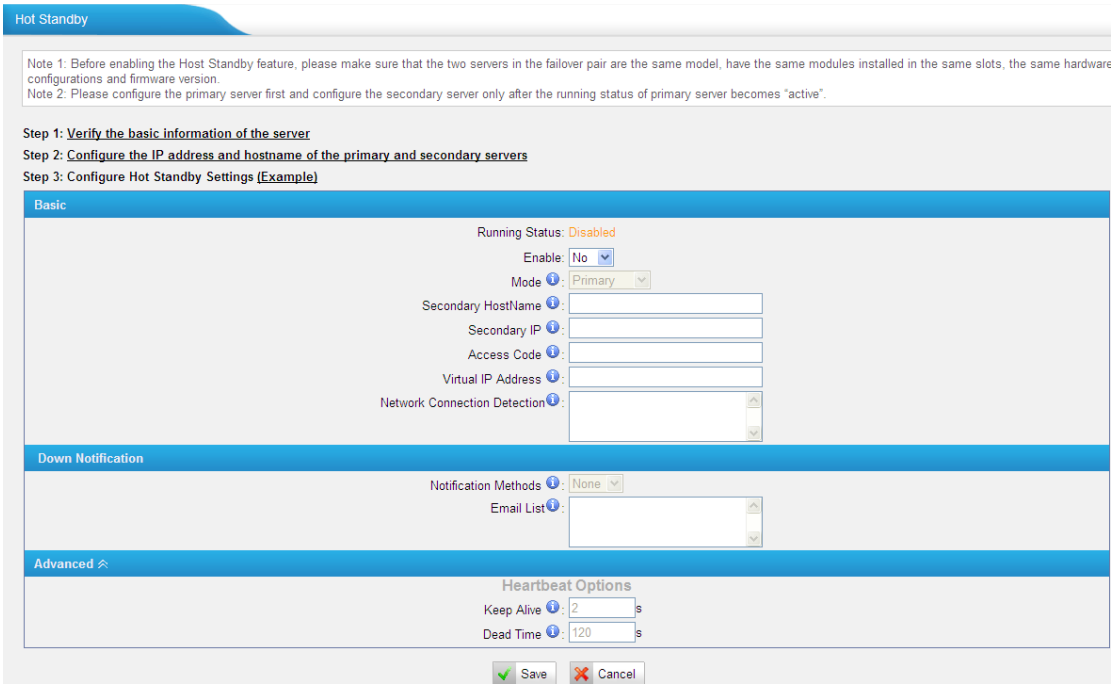

Hot Standby
Note 1: Before enabling the Host Standby feature, please make sure that the two servers in the failover pair are the same model, have the same modules installed in the same slots, the same hardware configurations and firmware version.
Note 2: Please configure the primary server first and configure the secondary server only after the running status of primary server becomes "active".
Step 1: Verify the basic information of the server
Step 2: Configure the IP address and hostname of the primary and secondary servers
Step 3: Configure Hot Standby Settings (Example)
Basic
Running Status: Disabled
Enable: No
Mode: Primary
Secondary HostName:
Secondary IP:
Access Code:
Virtual IP Address:
Network Connection Detection:
Down Notification
Notification Methods: None
Email List:
Advanced
Heartbeat Options
Keep Alive: 2 s
Dead Time: 120 s
Save
Cancel

Figure 5-15

**Mode**: Primary means the main unit; Secondary means the standby unit;

**Secondary/Primary Hostname**: If this unit mode is primary, then you need to input the hostname of standby unit; vise versa, if this unit is selected as secondary, then the hostname of primary unit is required. In brief, you need to input each other's host name on this field.

**IP**: You need to input each other's IP address on this field.

**Access code**: To make an identification number to verify each other. The number must be the same to both units.

**Virtual IP address**: To fill in a virtual IP address includes mask, which is always points to the currently activated unit. Customer can register IP phones through this virtual IP address. Please make sure the virtual IP add includes mask is the same on both units but different from their former IP address.

**Network Connection Detection**: Generally it requires the IP address of the router or gateway that connects both units. mPBX will connect another unit through this IP address.

**Down Notification**: The way of informing customer that the system down.

**Keep Alive:** Every 2 seconds, a package will be sent from one unit to another, which can test whether they are working properly.

**Dead Time:** The default setting is 120 seconds. If there's no response within 120s after one receiving a package from the other, then the normal working unit will figure the other unit is dead and send an email to report the failure.

## 5.3.5 Backup and Restore

We can backup up the configurations before reset WELL mPBX-U110R to factory defaults, and then restore it using this package.

**Note:**

1. Only configurations, custom prompts will be backed up, the voicemail and recording files are not included.
2. When you have update the firmware version, it's not recommend to restore using old package.

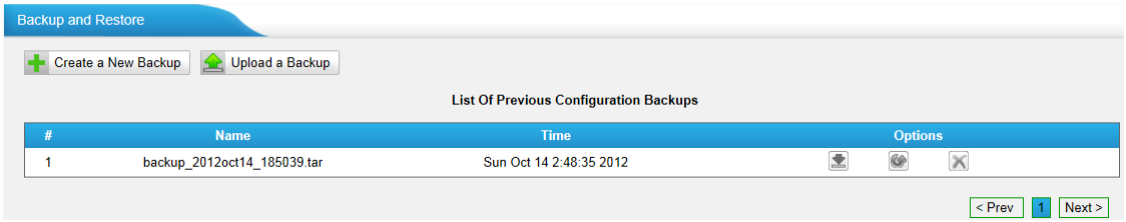

Backup and Restore
Create a New Backup
Upload a Backup
List Of Previous Configuration Backups
# Name Time Options
1 backup_2012oct14_185039.tar Sun Oct 14 2:48:35 2012
< Prev 1 Next >

Figure 5-16

## 5.3.6 Reset and Reboot

We can reset or reboot WELL mPBX-U110R via web directly in this page .

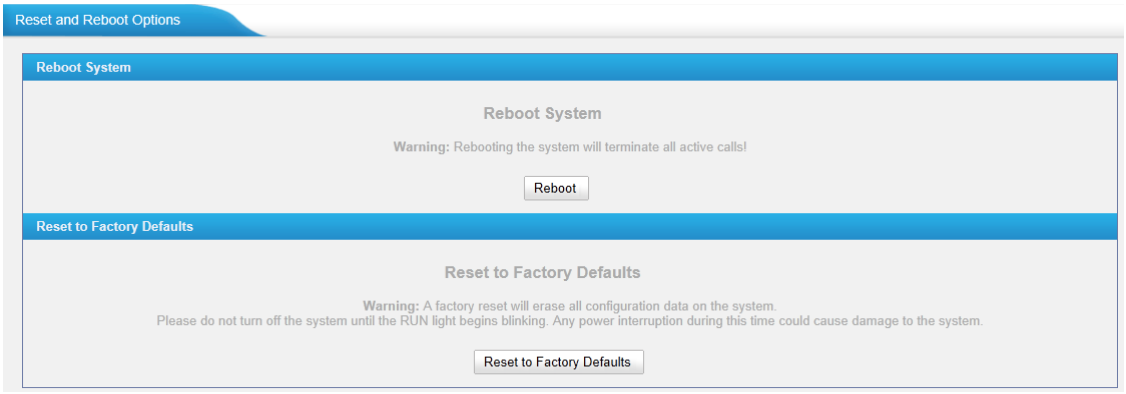

Reset and Reboot Options
Reboot System
Reboot System
Warning: Rebooting the system will terminate all active calls!
Reboot
Reset to Factory Defaults
Reset to Factory Defaults
Warning: A factory reset will erase all configuration data on the system.
Please do not turn off the system until the RUN light begins blinking. Any power interruption during this time could cause damage to the system.
Reset to Factory Defaults

Figure 5-17

**·Reboot System**

**Warning**: Rebooting the system will terminate all active calls!

**·Reset to Factory Defaults**

**Warning**: A factory reset will erase all configuration data on the system. Please do not turn off the system until the RUN light begins blinking. Any power interruption during this time could cause damage to the system.

## 5.3.7 Alert Settings

If the device is attacked, the system will notify users the alert via call or E-mail. The attack mode includes IP attack and Web Login.
More details for the system security configuration please refer to **APPENDIX G mPBX Security Configuration Guide.**

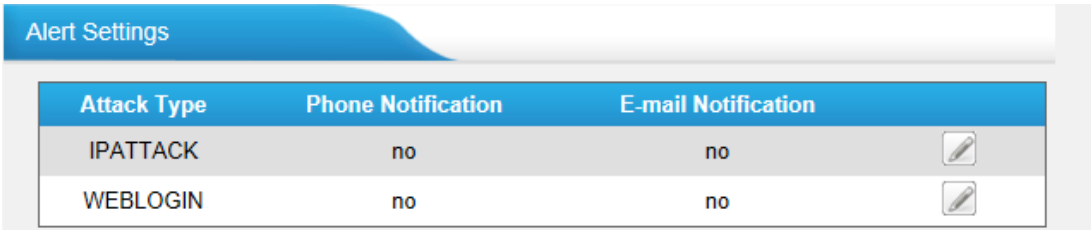



Figure 5.3.7.1

**IPATTACK**
When the system is attacked by an IP address, the firewall will add the IP to auto IP Blacklist and notify the user if it matches the protection rule.
**Note:** Please ensure that all voicemail settings are properly configured on the System Settings -> Voicemail Settings page before using Emails alert.

1) Phone Notification Settings

**·Phone Notification:**
Enable or disable phone notification

**·Number**
The numbers to call sending alert notification. Users can setup multiple extensions and outbound phone numbers. Please separate them by ‘;’. e.g. ‘500;81234’. If the extension has configured Follow Me Settings, the call would go to the forwarded number directly.

**·Attempts**
The attempts to dial the Number when there is no answer.

**·Interval**
The interval between each attempt to dial the phone number. Must be greater than 3 seconds
**·Prompts**

2) E-mail Notification Settings

**·E-mail Notification**
Enable or disable email notification

**·To**

Multiple mail address are allowed; please separate them by ';', e.g. 123@gmail.com;456@hotmail.com.

**·Subject**

The subject of email

**·Content**

Text content, support for predefined variables, Variable names and corresponding instructions are as follows:

$(HOSTNAME) host name

$(LOCALIP) local IP address

$(SOURCEIP) attack source IP address

$(DESTMAC) attacks destination mac (IPATTACK effective)

$(DESTPORT) attacks destination port number (IPATTACK effective)

$(PROTOCOL) protocol type (IPATTACK effective)

$(DATETIME) occurred

$(USERNAME) user name (WEBLOGIN effective)

$(INTERFACE) network interface name (IPATTACK effective)

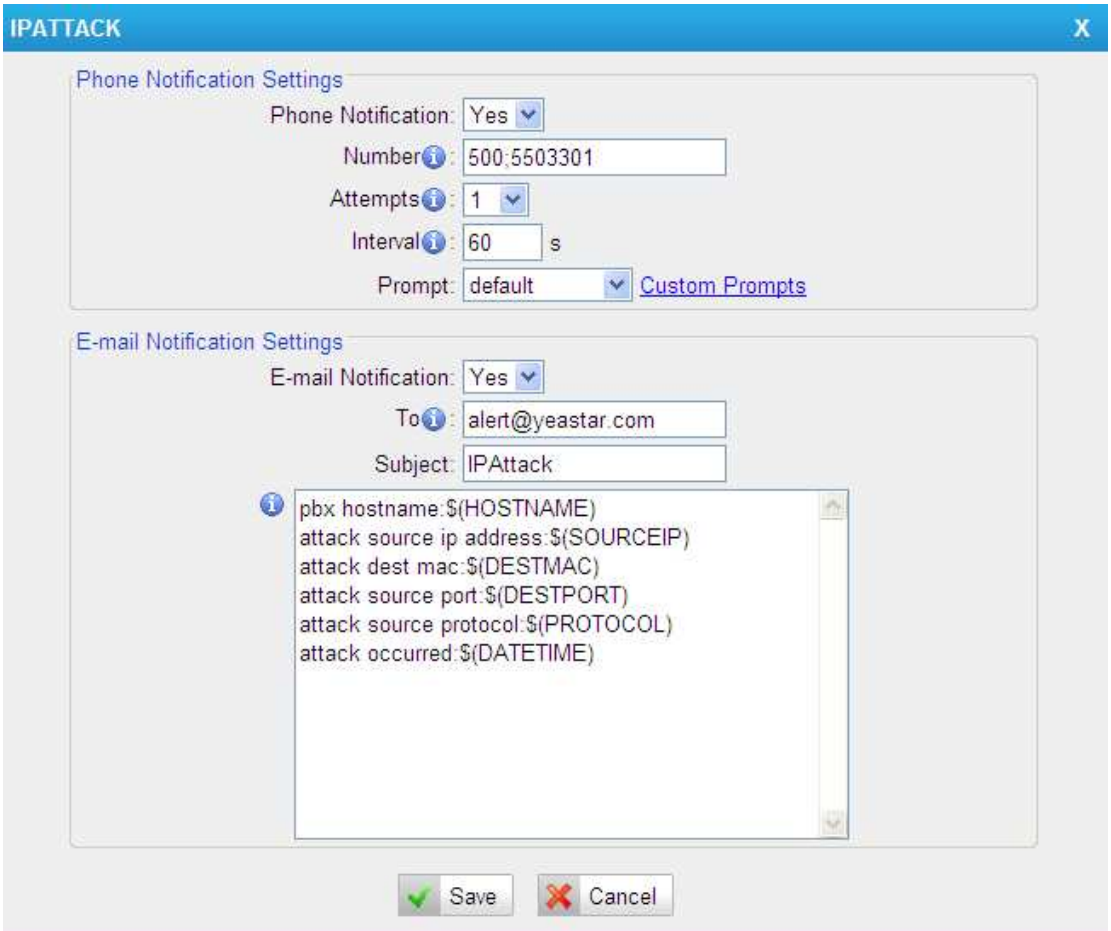



Figure 5.3.7.2

**WEBLOGIN**

Enter the password incorrectly five times to login mPBX interface will be regarded as attack. The system will limit the IP login within 10 minutes and notify the user.

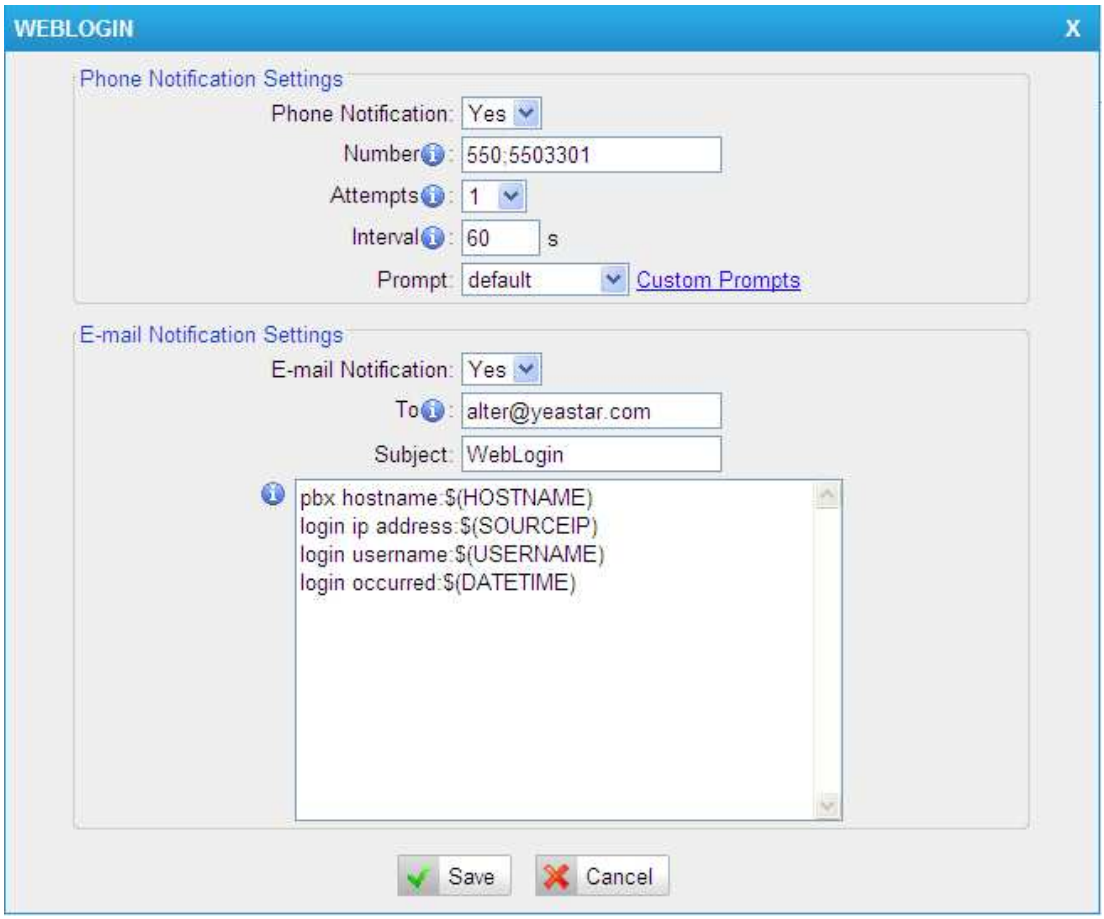



Figure 5.3.7.3

## 5.3.8 Addons

Call Recording enables all your inbound and outbound phone calls to be recorded. The system would detect any call conversation and record them automatically. The call recordings would be saved in the folder you specify and stored in the USB.

And if users want to use the function call recording, they need active this function firstly.

**Note:** For usage of the addon feature, please purchase activation code from your equipment provider.

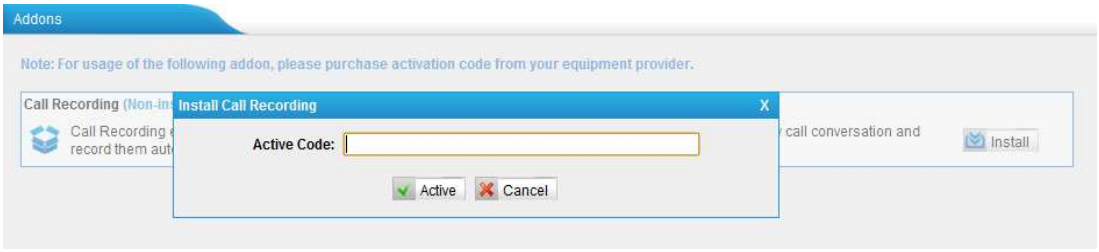



Figure 2.3.8.1

After activation, the page will show as below:

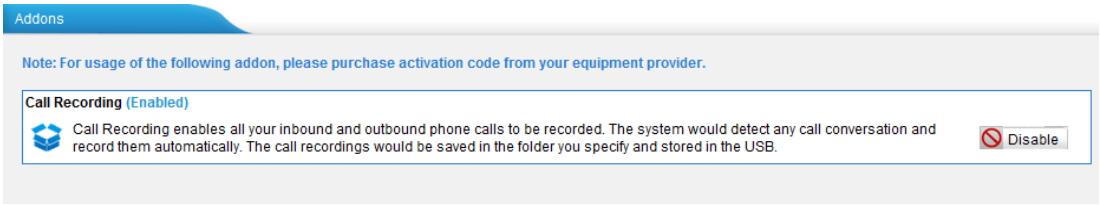

Addons
Note: For usage of the following addon, please purchase activation code from your equipment provider.
Call Recording (Enabled)
Call Recording enables all your inbound and outbound phone calls to be recorded. The system would detect any call conversation and record them automatically. The call recordings would be saved in the folder you specify and stored in the USB.
Disable

Figure 2.3.8.2

# 5.4 Storage Management

## 5.4.1 External Storage

The External Storage feature is used to extend storage space. Once configured, the files (voicemail, call recording files) created before the configured days will be moved to the Net-Disk.

**Note**: The shared folder must be based on Windows operation system.

Before external storage can be properly configured, an SMB share folder accessible from mPBX must be set up on a Windows based machine. Once that has been set up, please follow the steps below.

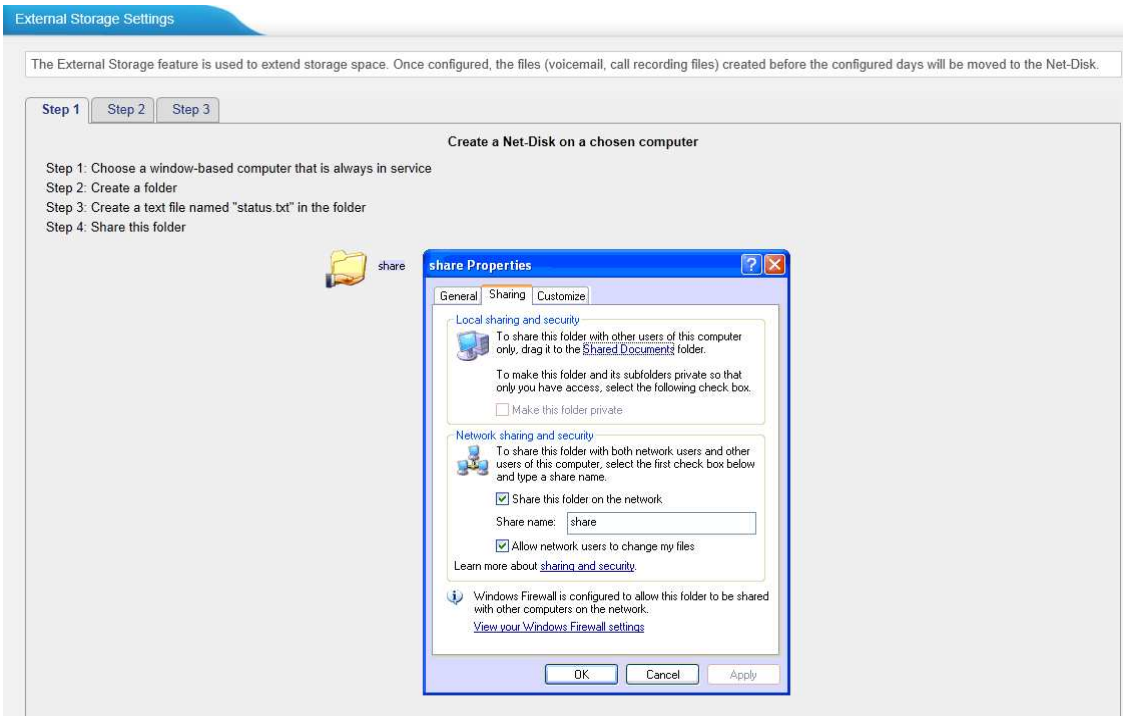

External Storage Settings
The External Storage feature is used to extend storage space. Once configured, the files (voicemail, call recording files) created before the configured days will be moved to the Net-Disk.
Step 1
Step 2
Step 3
Create a Net-Disk on a chosen computer
Step 1: Choose a window-based computer that is always in service
Step 2: Create a folder
Step 3: Create a text file named "status.txt" in the folder
Step 4: Share this folder
share
share Properties
General
Sharing
Customize
Local sharing and security
To share this folder with other users of this computer only, drag it to the Shared Documents folder.
To make this folder and its subfolders private so that only you have access, select the following check box.
Make this folder private
Network sharing and security
To share this folder with both network users and other users of this computer, select the first check box below and type a share name.
Share this folder on the network
Share name: share
Allow network users to change my files
Learn more about sharing and security.
Windows Firewall is configured to allow this folder to be shared with other computers on the network.
View your Windows Firewall settings
OK
Cancel
Apply

Figure 5-18

**Step 1**: Choose a window-based computer that is always in service
**Step 2**: Create a folder
**Step 3**: Create a text file named "status.txt" in the folder
**Step 4**: Share this folder

Then we need input the Net-Disk information in step2 page.

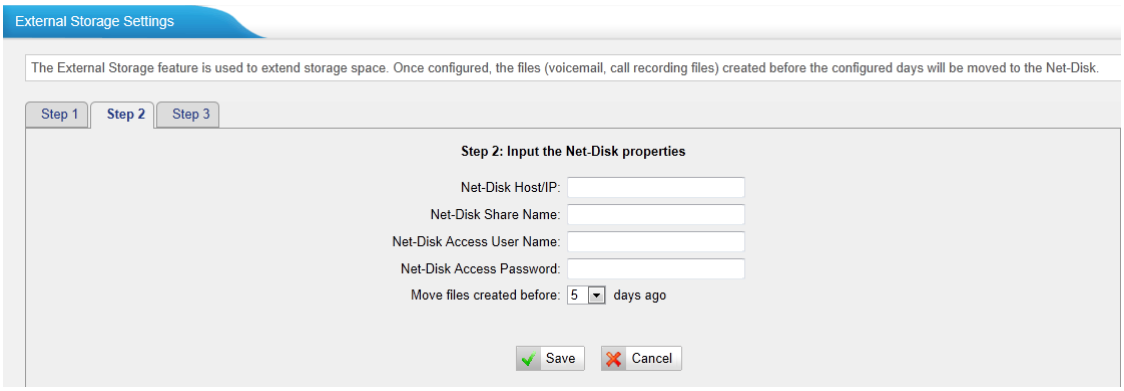

External Storage Settings
The External Storage feature is used to extend storage space. Once configured, the files (voicemail, call recording files) created before the configured days will be moved to the Net-Disk.
Step 1
Step 2
Step 3
Step 2: Input the Net-Disk properties
Net-Disk Host/IP:
Net-Disk Share Name:
Net-Disk Access User Name:
Net-Disk Access Password:
Move files created before: 5 days ago
Save
Cancel

Figure 5-19

**Net-Disk Host/IP**:Change this to the IP address of the computer where backup files will be stored.

**Net-DiskShare Name**: Change this to the name of the shared folder where backups will be stored.

**Net-DiskShare Username**: The user name used to log into the network share. Leave this blank if it is not required

**Net-DiskShare Password**: The password used to log into the network share.Leave this blank if it is not required

If configuringis correctly, open your Windows share folder to see if the mPBX backup files and folders has been created.If the contents of the backup folder look similar to step3 page, then you have successfully configured external storage on the mPBX unit.

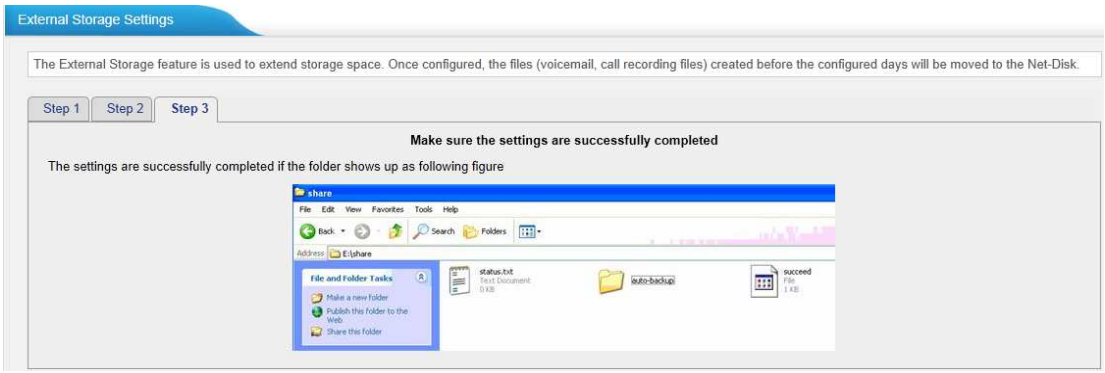

External Storage Settings
The External Storage feature is used to extend storage space. Once configured, the files (voicemail, call recording files) created before the configured days will be moved to the Net-Disk.
Step 1
Step 2
Step 3
Make sure the settings are successfully completed
The settings are successfully completed if the folder shows up as following figure
share
File Edit View Favorites Tools Help
Back Search Folders
Address E:\share
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
status.txt
auto-backup
succeed

Figure 5-20

# 6 PBX

Click

to access

In this page, we can configure the settings of extension, trunk, inbound call control, outbound call control, audio settings and the others. When configured well, we can make calls as scheduled

## 6.1 Extensions

In this page, we can configure the extensions' details and provision the supported models automatically.

### 6.1.1 FXS/VoIP Extensions

There are three types of extensions supported in WELL mPBX-U110R: SIP, IAX and analog extension.

**Note:**

1. The number of SIP/IAX extension is 100
2. The number of FXS extension is only 2 ( fixed)

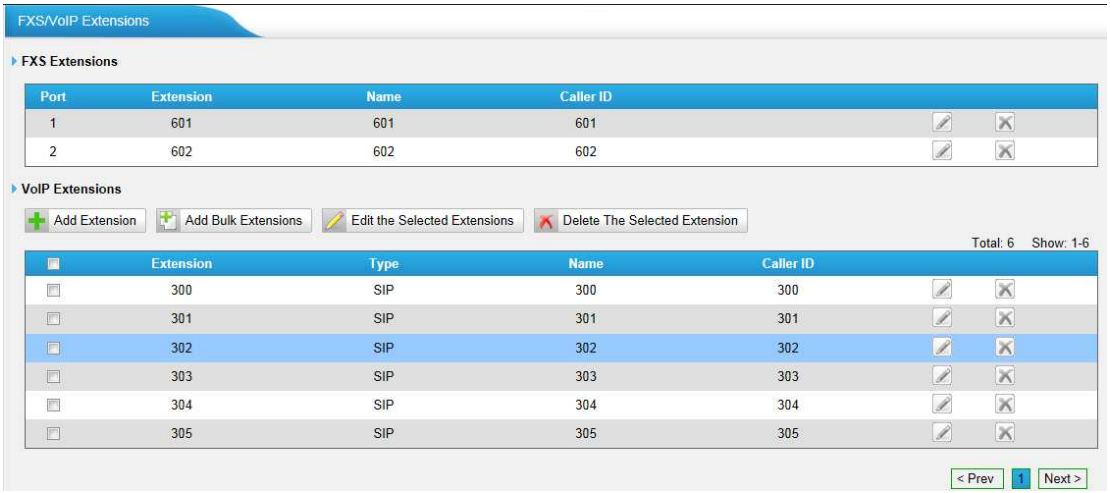



Figure 6-1

## FXS Extensions

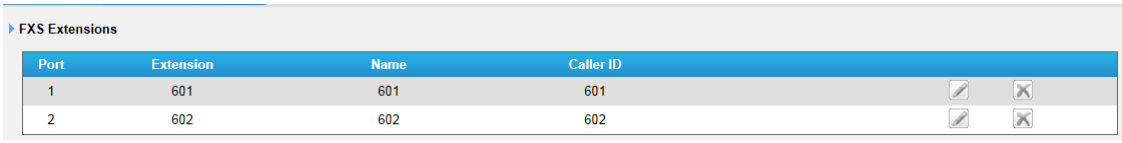



Figure 6-2

There are two fixed analog extensions in WELL mPBX-U110R, to modify the extension number, please delete it first, then recreate it again

1) General

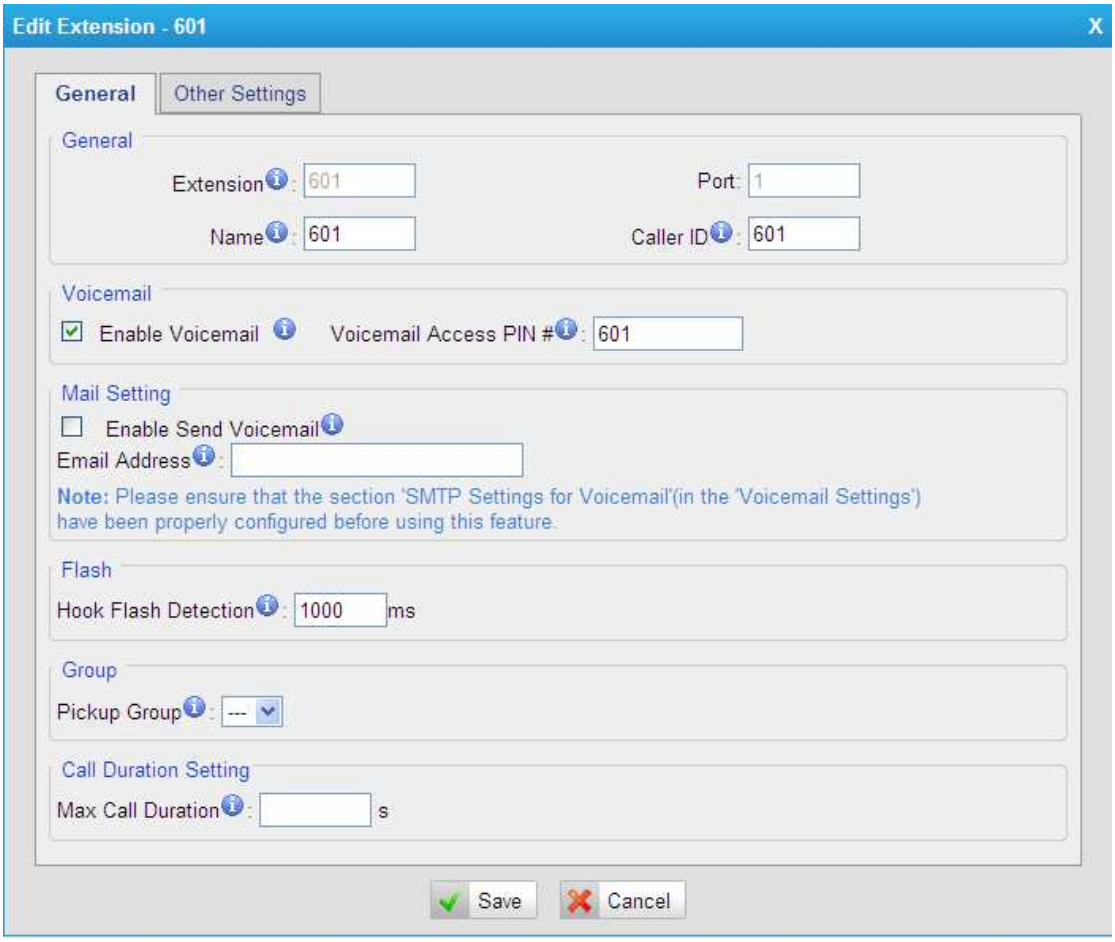



Figure 6-3

**·Extension**

The numbered extension, i.e. 1234, that will be associated with this particular User / Phone.

**·Port**

The extension correspond port.

**·Name**

A character-based name for this user, i.e. 'Bob Jones' .

**·Caller ID**

The Caller ID (CID) string will be used when this user calls another internal user.

2) Voicemail

**·Enable Voicemail**

Check this box if the user should have a voicemail account.

**·Voicemail Access PIN #**

Voicemail Password for this extension, i.e. '1234'.

3) Mail Setting

**·Enable Send Voicemail**

Once enabled, the voicemail will be sent to the belowemail address as an attachment.

**·Send Voicemail to Email Address**

This option defines whether or not voicemails/Fax is sent to the Email address asan attachment.

**Note**: Please ensure that all voicemail settings are properly configured on the System Settings -> Voicemail Settings page before using this feature.

4) Flash

**·Hook Flash Detection**

Sets the amount of time, in milliseconds, that must pass since the last hook-flash event received by mPBX before it will recognize a second event. If a second event occurs in less time than defined byHook Flash Detection, then mPBX will ignore the event. The default value of Flash is 1000 ms, and it can be configured in 1ms increments.

5) Group

**·Pickup Group**

If this extension belongs to a pickup group, any calls that ring this extension can be picked up by other extensions in the same pickup group by dialing the Call Pickup feature code (default *4).

**Note**: *4 is the default setting, it can be changed under Feature Codes -> General -> Call Pickup.

6) Call Duration Settings

Setup the max cull duration for every call of this extension, but it's only valid for outbound calls. And if enter '0' or leave this blank empty, the value would be equal to the max call duration configured in the Option Settings page.

Note: This setting will not be valid for internal calls.

7) Other options

**·Call Waiting**

Check this option if the extension should have Call Waiting capability.If this option is checked, the 'When busy' follow me options will not be available.

**·DND**

Don't Disturb.

**·User Web Interface**

Check this option to allow the user to login to the mPBX User Web interface, which can be used to access voicemail and extension recordings. Users may login to the mPBX User Web interface by using their extension number and voicemail PIN # as the login and password respectively.

**·Ring Out**

Check this option if you want to custom the ring time. Tone will stop over the time defined

8) Follow me (Call Forwarding)

This function sets inbound call forwarding on an extension. An administrator can configure Follow Me for this extension

9) Volume Settings

Rxgain: The Volume sent to FXS extension.

Txgain: The Volume sent out by the FXS extension

10) Mobility Extension

mPBX allows you to use your mobile phone as extension. If you set your mobile phone as mobility extension and then you call mPBX with this mobility phone, you will hear a dial tone. mPBX will recognize your call as a call from an extension. You can dial the number of other extensions (Your caller ID will be the number of your extension) or dial out via outbound routes just like dialing from your extension.

**Note**: If callback is enabled in the inbound route, the mobility extension function of this inbound route will be disabled

11) Spy Settings

mPBX allows extension to monitor/barge in other conversation. Once this feature is enabled, the extension has the ability to monitor/barge in other calls using the feature codes for each spy mode, refer to 'Feature Codes' page for more information.

**·spy modes**

There are 4 spy modes available for choice:
General spy: you have the permission to use the following 3 modes.
Normal spy: you can only hear the call, but can't talk
Whisper spy: you can hear the call, and can talk with the monitored extension
Barge spy: you can hear the call and talk with them both

**Note**: for example,if 500 want to monitor extension 501, we need to enable the 'allow being spied ' for 501, and choose the spy mode for extension 500. Then pick up 500 and dial "feature codes + 501" to start monitoring when 501 is in a call.

If 500 choose 'normal spy', it should dial'*90501' to start monitoring;
if 500 choose 'whisper spy', it should dial '*91501' to start monitoring;
if 500 choose 'barge spy', it should dial '*92501' to start monitor;
if 500 choose 'general spy', it can dial '*90501','*91501' or '*92501' to start monitor.

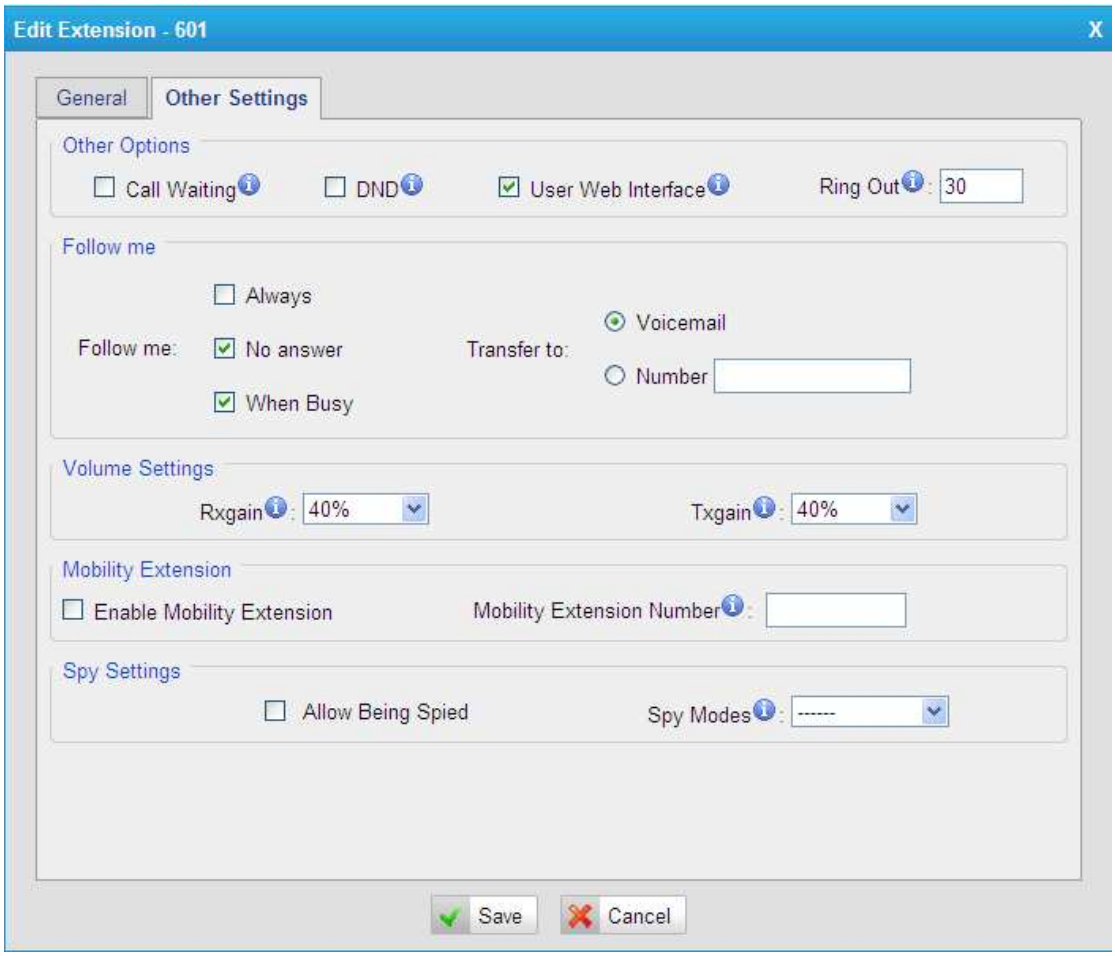



Figure 6-4

# VoIP Extensions

A VOIP extension is a SIP/IAX Account that allows an IP Phone or an IP Soft-Phone client to register on mPBX

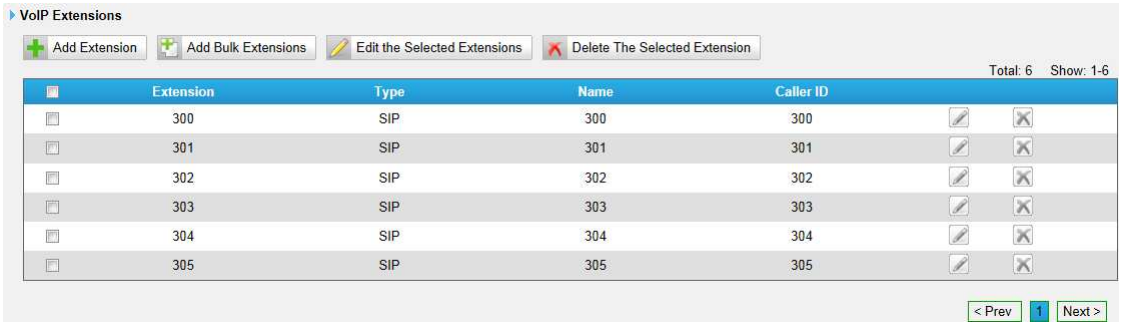



Figure 6-5

We can click 'Add extension' to start.

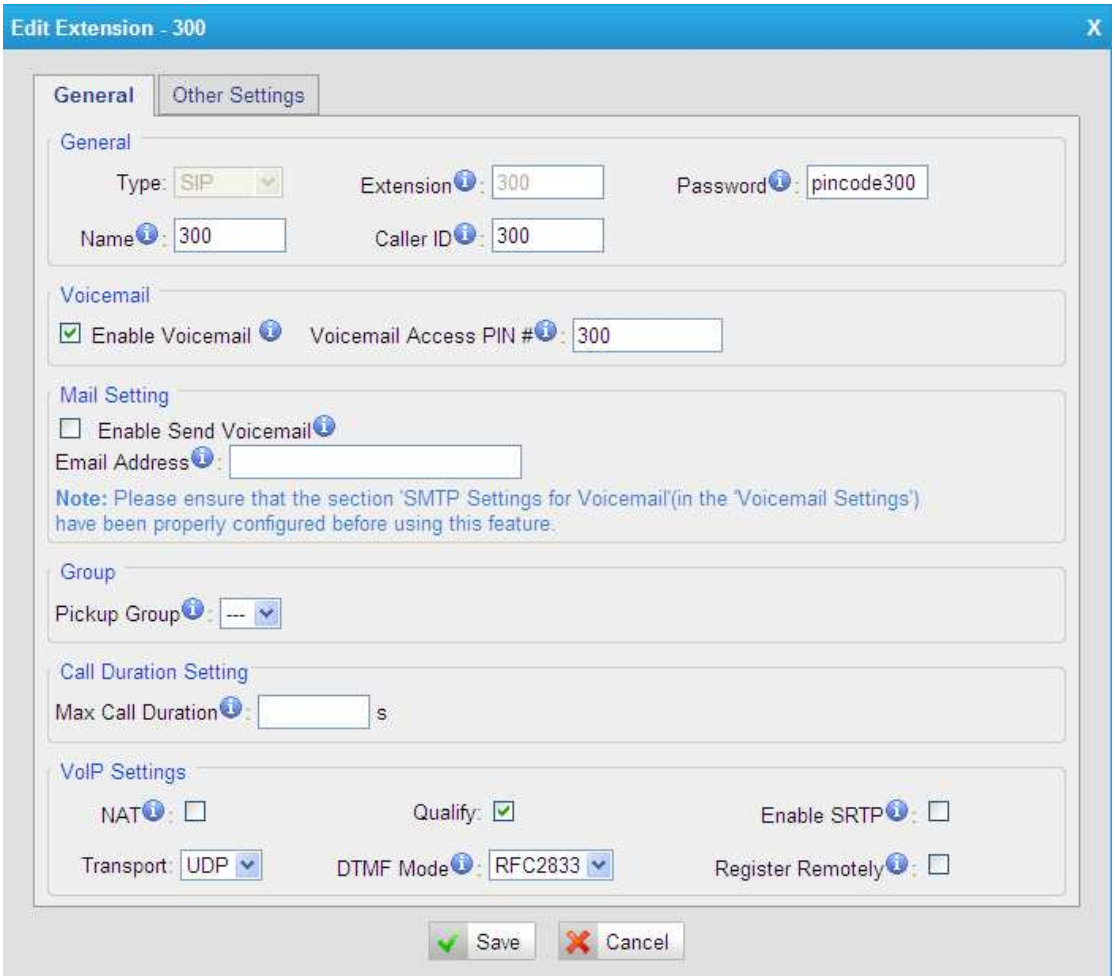



Figure 6-6

1) General

**·Type**

Extension type: SIP,IAX or SIP/IAX.

SIP – The extension sends and receives calls using the VoIP protocol SIP.
IAX -The extension sends and receives calls using the VoIP protocol IAX.

**·Extension**
The numbered extension, i.e. 1234, that will be associated with this particular User / Phone.

**·Password**
The password for this extension, Ex: '12t3f6'

**·Name**
A character-based name for this user, EX: 'Bob Jones'

**·Caller ID**
The Caller ID will be used when this user calls another internal extension.

2) Voicemail
**·Enable Voicemail**
Check this box if the user should have a voicemail account.

**·Voicemail Access PIN #**
The voicemail Password for this extension, i.e. '1234'.

3) Mail Setting
This option defines whether or not voicemails or faxes are sent to an Email Address as attachment.

**·Enable Send Voicemail**
Once enabled, the voicemail will be sent to email as an attachment.

**·Email Address**
Email address used to receive the voicemail or Fax.
**Note**: Please ensure that the section 'SMTP Settings For Voicemail'(in the 'Voicemail Settings') have been properly configured before using this feature.

4) Group
**·Pickup Group**
If this extension belongs to a pickup group, any calls that ring this extension can be picked up by other extensions in the same pickup group by dialing the Call Pickup feature code (default is*4).
**Note**: *4 is the default setting, it can be changed under Feature Codes -> General -> Call Pickup.

5) Call Duration Settings

Setup the max cull duration for every call of this extension, but it's only valid for outbound calls. And if enter '0' or leave this blank empty, the value would be equal to the max call duration configured in the Option Settings page.

Note: This setting will not be valid for internal calls.

6) VoIP Settings

**·NAT**

This setting should be used when the system is using a public IP address to communicate with devices hidden behind a NAT device (such as a broadband router). If you have one-way audio problems, you usually have problems with your NAT configuration or your firewall's support of SIP and/or RTP ports.

**·Qualify**

Send check alive packets to IP phones

**·Enable SRTP**

Enable extension for SRTP (RTP Encryption).

**·Transport**

This will be the transport method used by the extension. The options are UDP (default) or TCP or TLS.

**·DTMF Mode** – RFC2833, Info, Inband, Auto.

**·Remote Register**

Allow to register remote extensions.

This option is used to enhance the system security, it's disabled by default. More details for the system security configuration please refer to **APPENDIX G mPBX Security Configuration Guide**.

7) Other Options

**.Call Waiting**

Check this option if the extension should have Call Waiting capability. If this option is checked, the 'When busy' follow me options will not be available. The call waiting function of IP phone has higher priority than mPBX's call waiting function.

**.DND**

Don't Disturb. When DND is enabled for an extension, the extension will be not available.

**.User Web Interface**

Check this option to allow the user to login to the mPBX User Web interface,

which can be used to check voicemail and extension recordings. Users may login to mPBX User Web interface by using their extension number and voicemail PIN # as the login and password respectively.

**.Ring Out**

Check this option if you want to customize the ring time. Ring tone will stop over the time defined.

8) Follow me (Call Forwarding)

Call forwarding for an extension can be configured here. The administrator can configure Follow Me option for this extension. If you want to transfer the call to an outbound number, please follow the dial pattern of outbound route filled in the outbound number.

For example: transferring to your mobile phone number 123456789, the dial pattern of outbound route is '9.', you should fill in 9123456789 here.

9) IP Restriction

**·Enable IP Restriction**

Check this option to enhance the VoIP security for mPBX. If this option is enabled, only the permitted IP/Subnet mask will be able to register this extension number. In this way, the VoIP security will be enhanced.

**·Permitted 'IP address/Subnet mask'**

The input format should be 'IP address'+'/'+'Subnet mask'.

e.g."192.168.5.100/255.255.255.255" means only the device whose IP address is 192.168.5.100 is allowed to register this extension number.

e.g."192.168.5.0/255.255.255.0" means only the device whose IP address is 192.168.5.XXX is allowed to register this extension number.

10) Mobility Extension

mPBX allows you to use your mobile phone as extension. If you set your mobile phone as mobility extension and then you call mPBX with this mobility phone, you will hear a dial tone. mPBX will recognize your call as a call from an extension. You can dial the number of other extensions (Your caller ID will be the number of your extension) or dial out via outbound routes just like dialing from your extension.

**·Mobility Extension Number**

Don't forget to add the dial patterns of the outbound route at the beginning of your mobile phone number when you fill in the mobility extension number filed. E.g. if you want to set "15960XXXXXX" as mobile extension, and the dial pattern of the outbound route is "9"; you should set "915960XXXXXX" here.

**Note**: If callback is enabled in the inbound route, the mobility extension function of this inbound route will be disabled

11) Spy Settings

mPBX allows extension to monitor/barge in other conversation. Once this feature is enabled, the extension has the ability to monitor/barge in other calls using the feature codes for each spy mode, refer to 'Feature Codes' page for more information.

**·spy modes**

There are 4 spy modes available for choice:
General spy: you have the permission to use the following 3 modes.
Normal spy: you can only hear the call, but can't talk
Whisper spy: you can hear the call, and can talk with the monitored extension
Barge spy: you can hear the call and talk with them both

**Note**: for example,if 500 want to monitor extension 501, we need to enable the 'allow being spied ' for 501, and choose the spy mode for extension 500.
Then pick up 500 and dial "feature codes + 501" to start monitoring when 501 is in a call

If 500 choose 'normal spy', it should dial'*90501' to start monitoring;
If 500 choose 'whisper spy', it should dial '*91501' to start monitoring;
If 500 choose 'barge spy', it should dial '*92501' to start monitor;
If 500 choose 'general spy', it can dial '*90501','*91501' or '*92501' to start monitor.

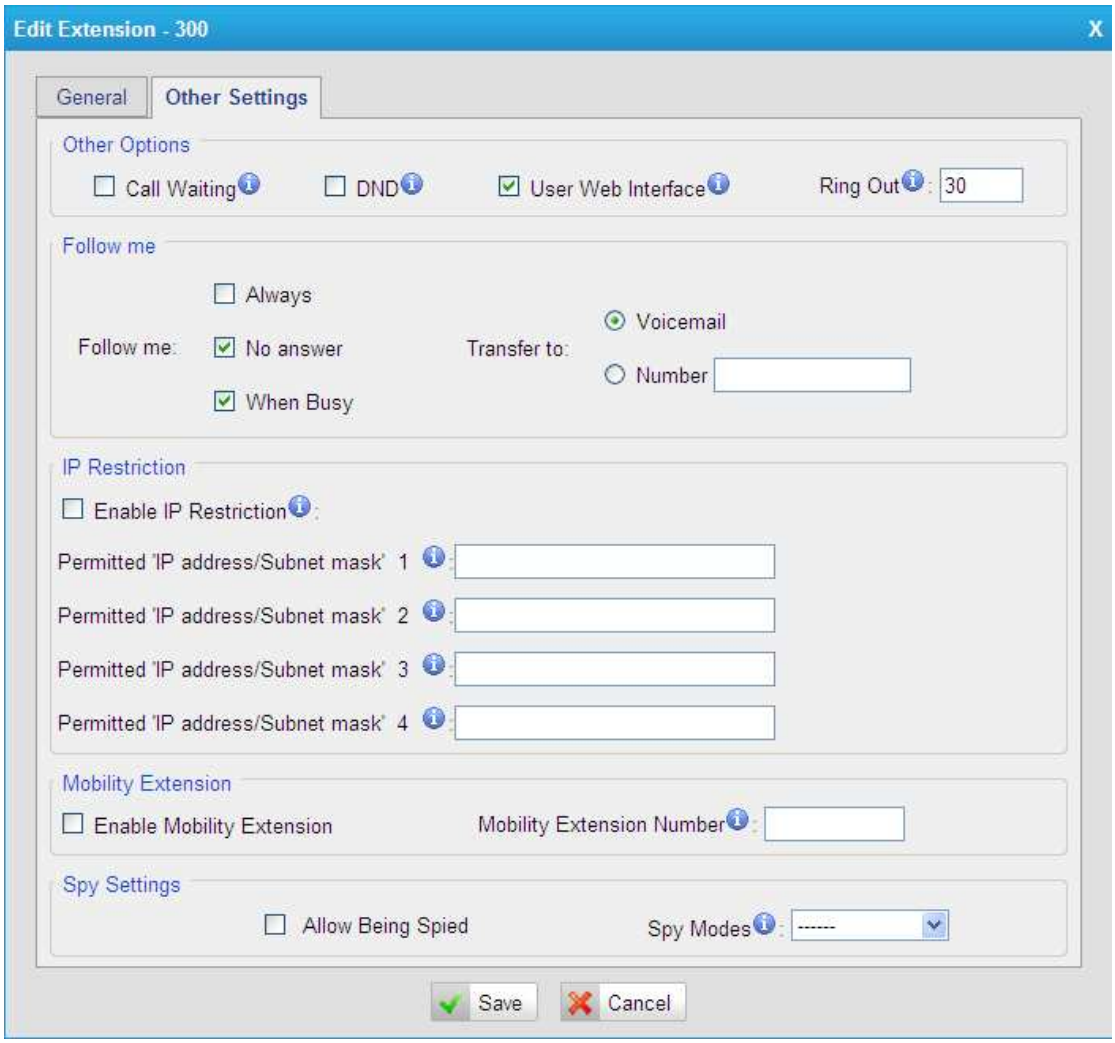



Figure 6-7

## 6.1.2 Phone Provisioning

The Auto Provision sub menu provides users a method to Auto Provision IP Phone after the Express Setup process.

**Note**: Auto Provision functions fully test with these models:

Yealink (T12,T18,T20,T22,T26,T28,T32,T38,VP530,VP-2009)

Snom ( 300,320,360,370)

Polycom (IP 6000,IP 7000,IP 32X,IP33X,IP430,IP450,IP550,IP560,VVX1500)

Cisco (IP7940,IP7960)

Aastra(480i,480i CT,6757i,6757i CT, 6737i)

Grandstream(GXP1450,GXP2100,GXP2110,GXP2120)

Escene(ES220,ES320,ES330,ES410,ES620)

Fanvil(C56,C58,C60,C62)

**News:**

**When provisioning Yealink and Snom IP phone, mPBX is not needed to be set as the only DHCP server any more**

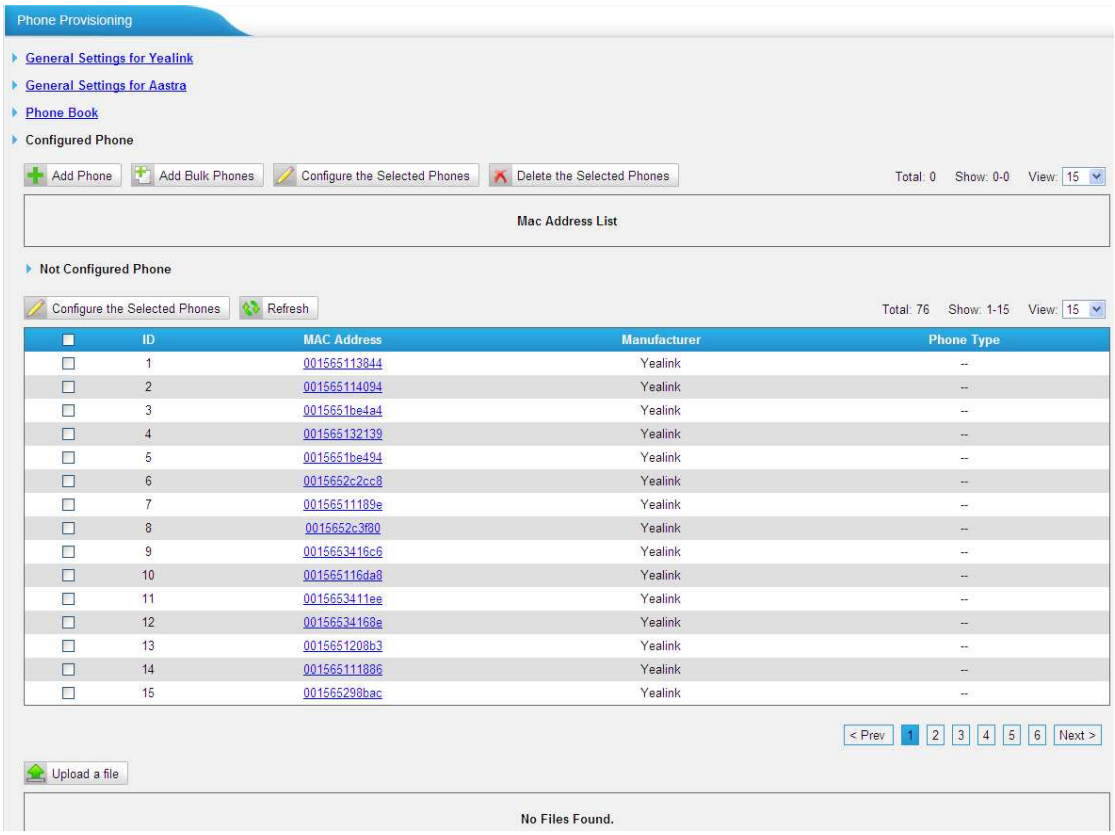



Figure 6-8

### 6.1.2.1 General Settings for Yealink

In this page, you can configure it before provisioning Yealink IP phones, including the items like general preferences, codecs, remote phone book and firmware upgrade

**Note**: if firmware download server is enabled, IP phone will update the firmware automatically according the version and server you have configured during the provision process.

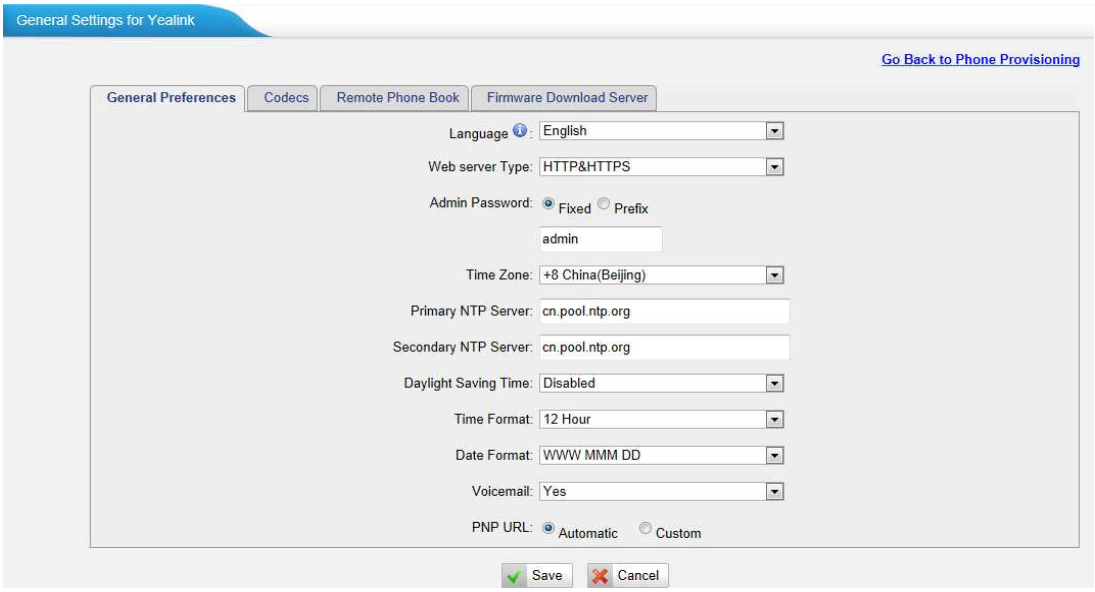



Figure 6-9

### 6.1.2.2 General Settings for Aastra

In this page, you can configure it before provisioning Aastra IP phones, including the items like local dial plan, time and date setting programkeys configuration and so on.

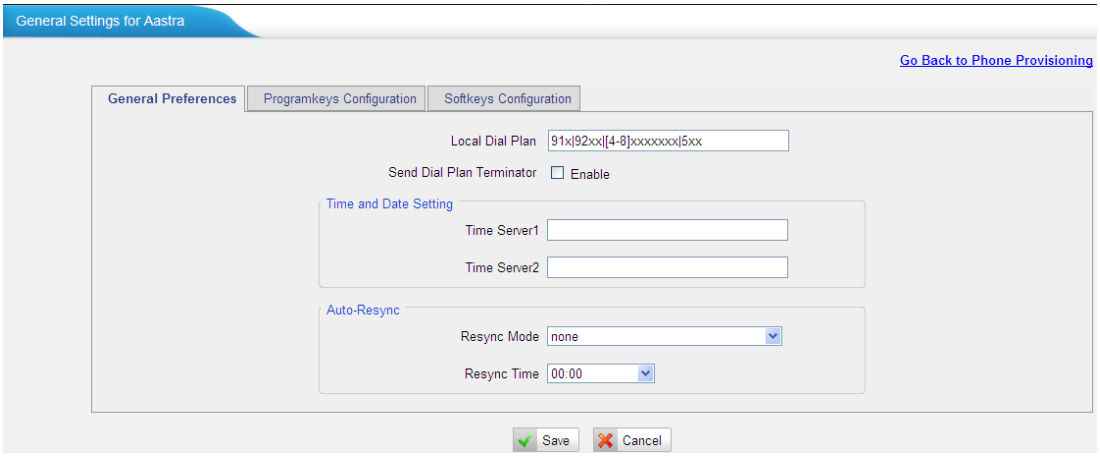



Figure 6-10

### 6.1.2.3 Phone book

You can add your contacts here and provision them to your IP phone

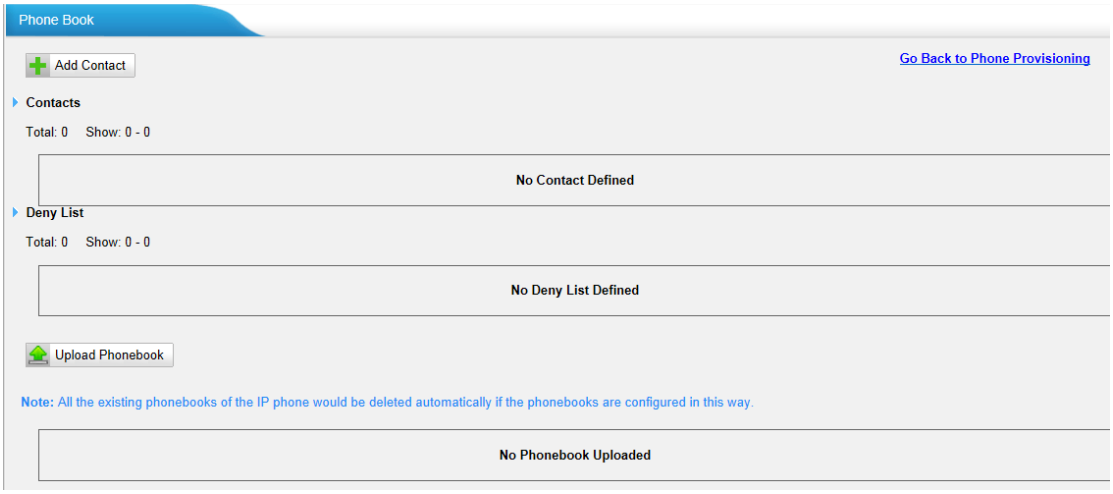

Phone Book
Add Contact
Go Back to Phone Provisioning
Contacts
Total: 0 Show: 0 - 0
No Contact Defined
Deny List
Total: 0 Show: 0 - 0
No Deny List Defined
Upload Phonebook
Note: All the existing phonebooks of the IP phone would be deleted automatically if the phonebooks are configured in this way.
No Phonebook Uploaded

Figure 6-11

1) Add Contact

**·Type**

There are three types: None, VIP and Deny list (Blacklist).

**·Group**

There are 5 groups: None, Friends, Family, Work, Colleagues list.

**·Nick Name**

You can set a nick name for this number.

**·Favorite**

Only works with snom phone.

**·Organization**
Input the organization of this contact. Only works with snom phone.

**·Title**
Input the title of this contact. Only works with snom phone.

**·Email**
Input the email of this contact. Only works with snom phone.

**·Birthday**
Input the birthday of this contact. Only works with snom phone.

**·First Name**
Input the first name of this contact. Only works with snom phone.

**·Family Name**
Input the family of this contact. Only works with snom phone.

**·Office Number**
Input the office number here

**·Mobile Number**
Input the mobile number here

**·Home Number**
Input the home number here

**·Sub Number**
Add sub number of this contact. Only works with snom phone.

**·Note**
Take some note of this contact. Only works with snom phone.

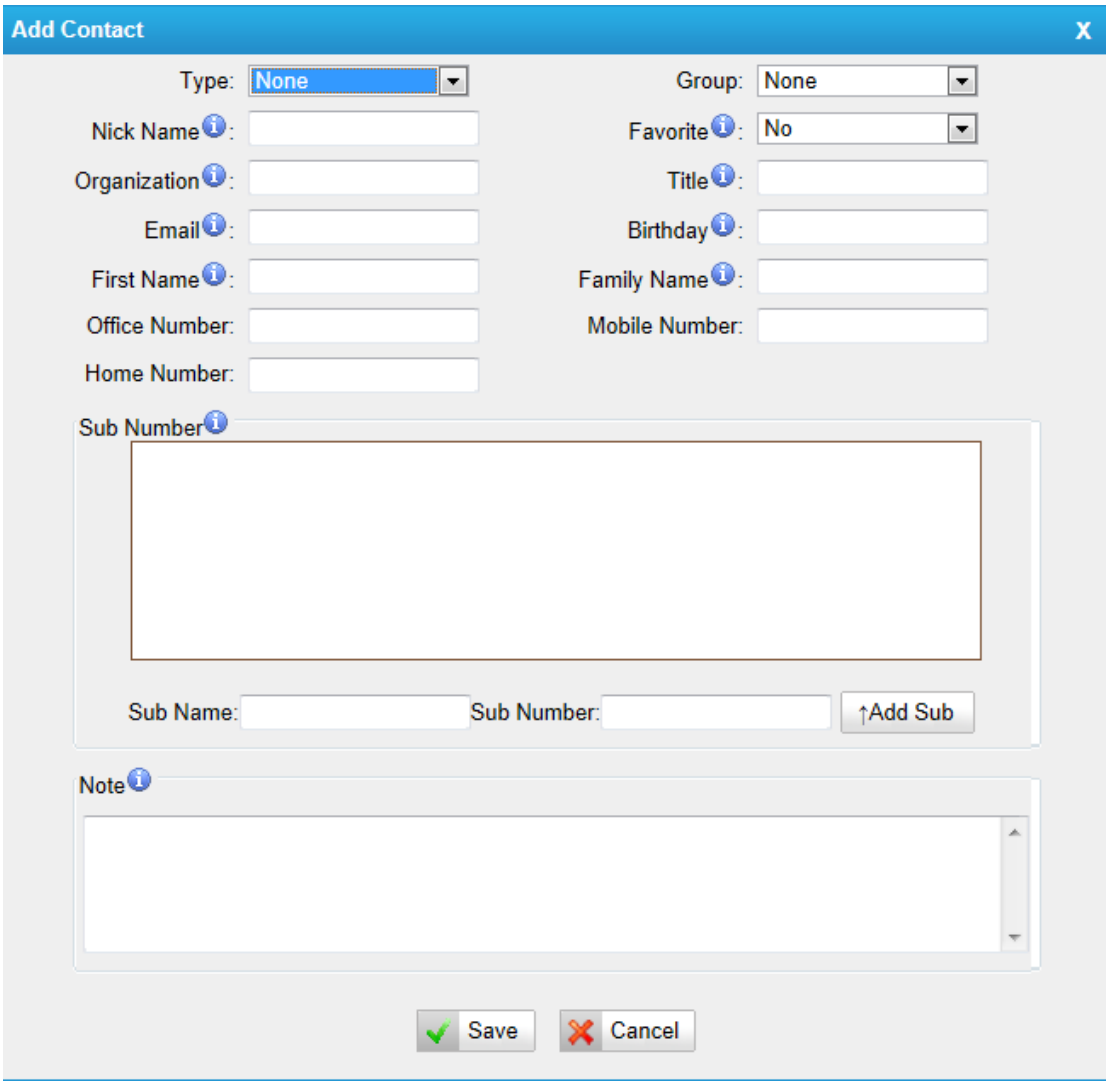



Figure 6-12

2) Upload Phonebook

You can upload a phonebook before auto provision, which will be provisioned to the IP phone when using auto provision feature to configure your IP phones. The format of phonebook should be *.xml.

**Note**:All the existing phonebooks of the IP phone will be replaced automatically if the phonebooks are configured in this way.

### 6.1.2.4 Configure phone

Let's take provisioning yealink as an example

Create New Phone have two modes,

Create New phone in webpage and Upload the IP Phone's configure file.

**Add new phone via webpage**

Click 'Add Phone' and fill in the corresponding information in the popup window

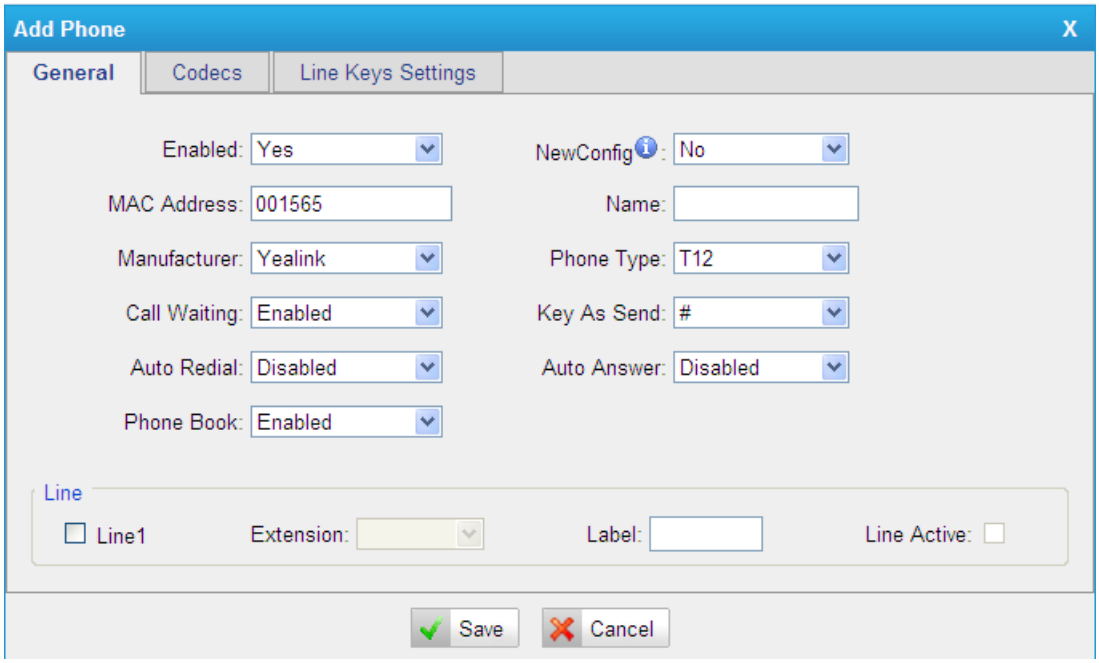



Figure 6-13

**1) General**

**· Enabled**

Choose yes or no to enable or disable this extension

**· NewConfig**

If the firmware version number is greater than or equal to 70,please enable this option.

**Note:** when choose the Manufacturer as Yealink, a special option 'NewConfig' need to be considered. If the firmware version number of the Yealink phone is bigger or equal to 70, please enable this option.

**· MAC address**

Input the MAC address of IP phone

**·Name**

Put the name of this Phone here.

**·Manufacturer**

You can choose the Manufacturer of IP phone

**·Phone Type**

Choose the model of your phone. Only for snom phone

**·Call Waiting**

This call feature allows your phone to accept other incoming calls to an extension already in an active call.

**·Key as Send**
Configure the key as send, you choose # ,* or disable it

**·Auto redial**
Enable the auto redial for IP Phone

**·Auto answer**
Configure if auto answer is allowed for IP phone

**·Phone book**
Enable the feature of phone book of IP phone

**2) Codecs**
In this page, we can set the codecs for Ip phone

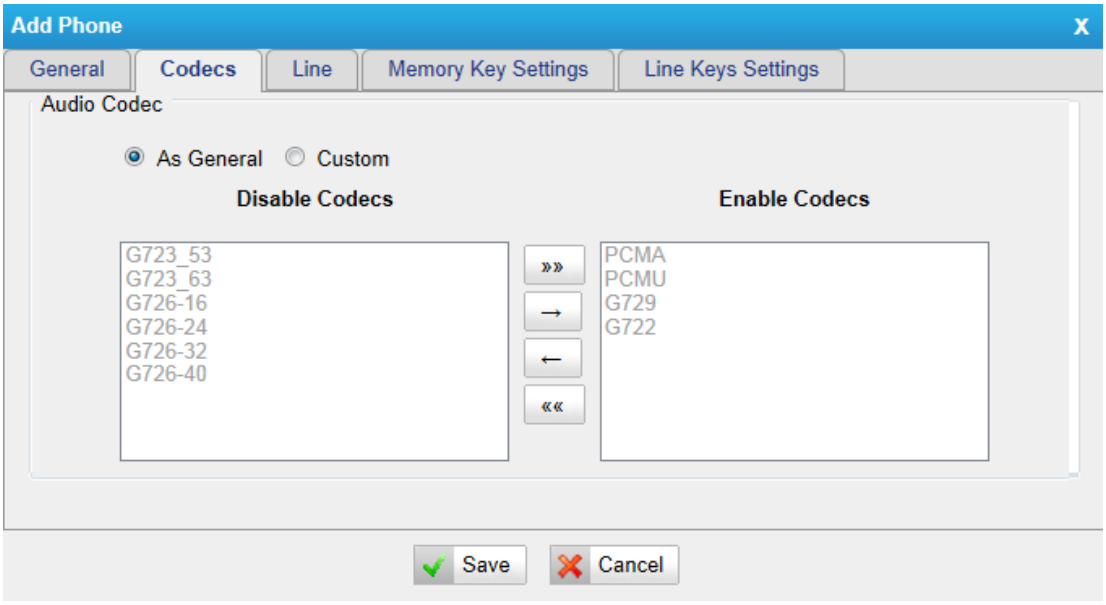



Figure 6-14

**3) Line**
In this page, we can set each line of IP phone for the account you want, active or not .

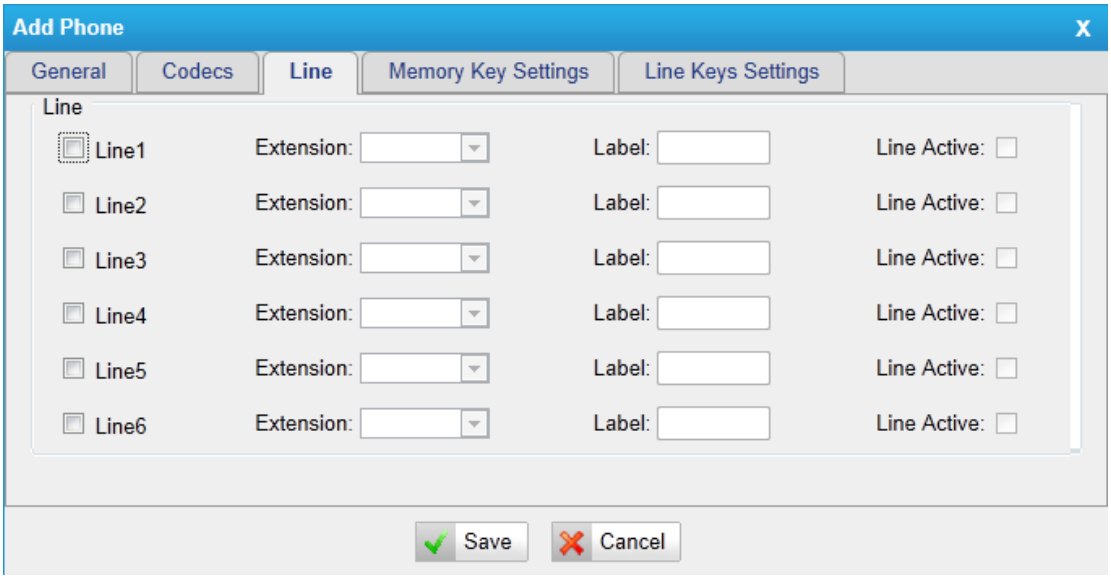



Figure 6-15

Extension: Selected the extension number for IP Phone.
Label: It is shown on the LCD for users to identify the account.
Line Active: You can choose on/off to enable/disable the account respectively

**4) Memory key settings**

In this page, we can configure the DSS keys of IP phone one by one .

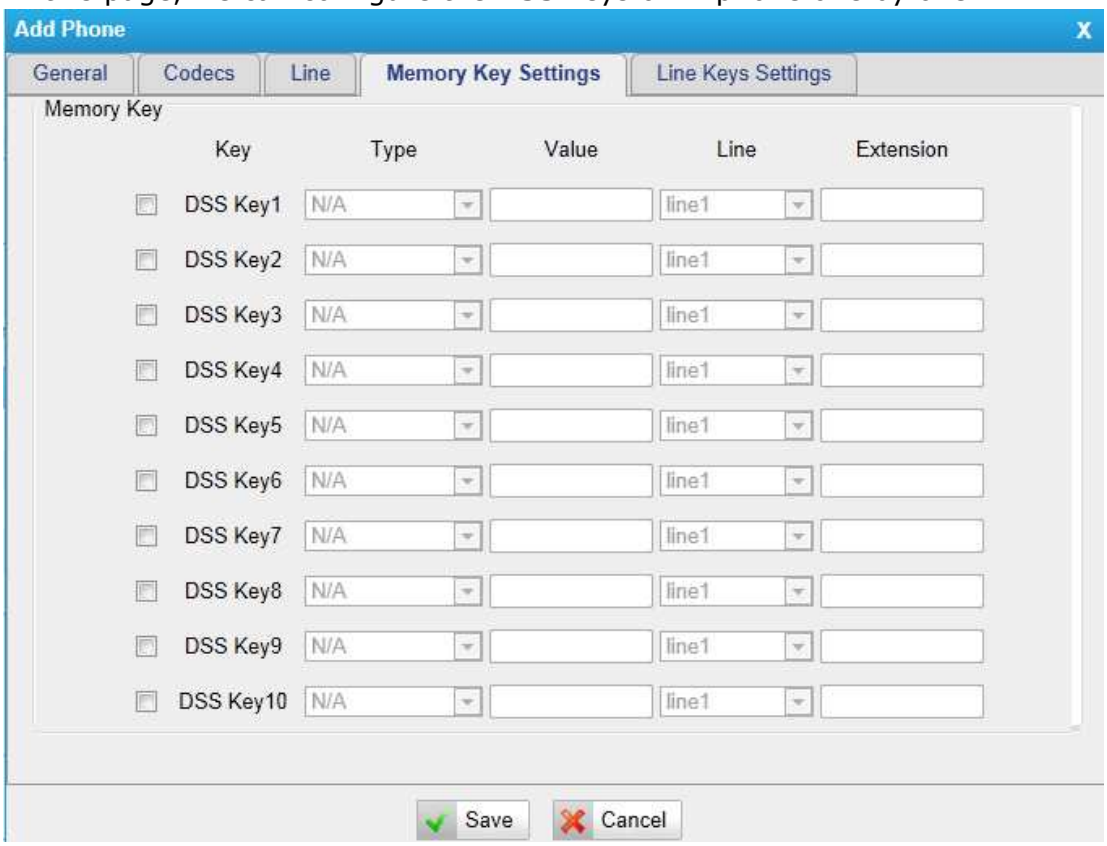



Figure 6-16

**5) Line keys settings**

We can configure the line key settings for this IP phone

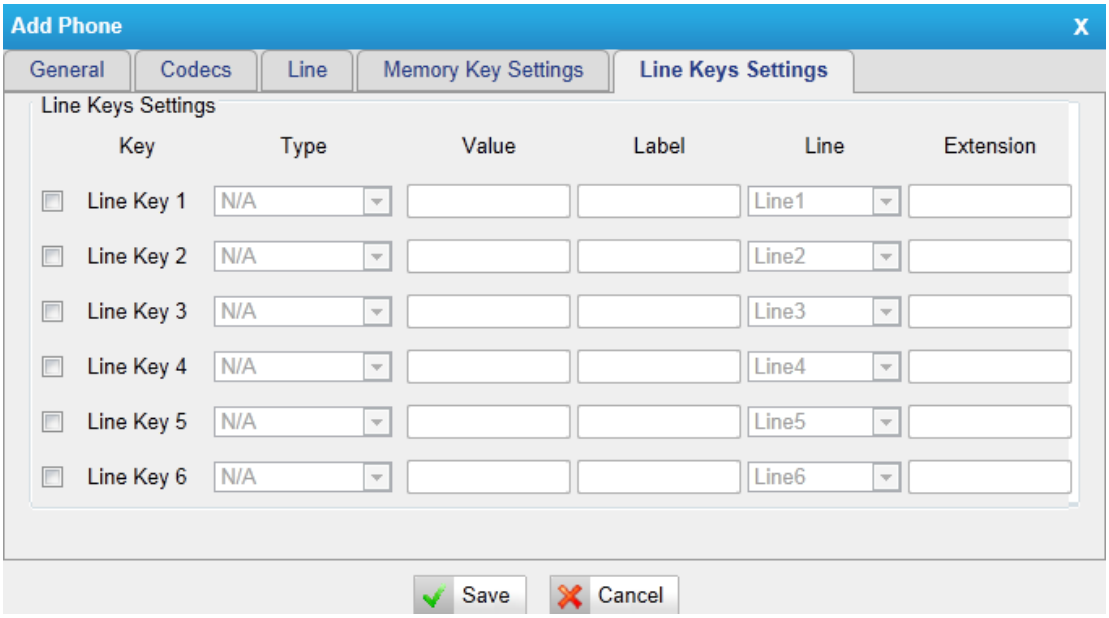



Figure 6-17

### 6.1.2.5 Not configured phone

In this section, mPBX will scan all the supported IP phones and display here, we can click the 'MAC address' of IP phone and input the corresponding information in the popup window, like the picture shows below

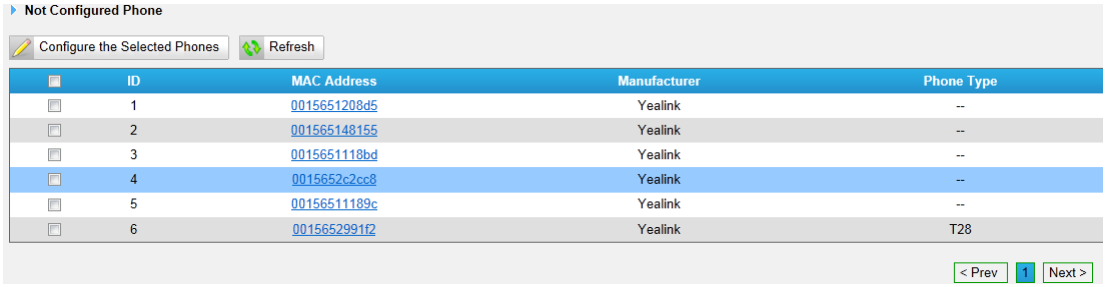



Figure 6-18

### 6.1.2.6 Upload a file

Click 'Upload a file' and choose the configure file of IP phonein the popup window.

**Note**: the file format must be .cfg

Please edit the configuration files in advance before uploading

Figure 6-19

# 6.2 Trunks

There are two types in WELL mPBX-U110R, the VOIP trunk and the E1 trunk, we cannot any other trunks like PSTN/GSM/BRI anymore.

## 6.2.1 Physical Trunk

In this page we can configure the details of E1 trunk, before configure anything, please make sure the cable is fine, and you have got enough information from the ISDN provider.

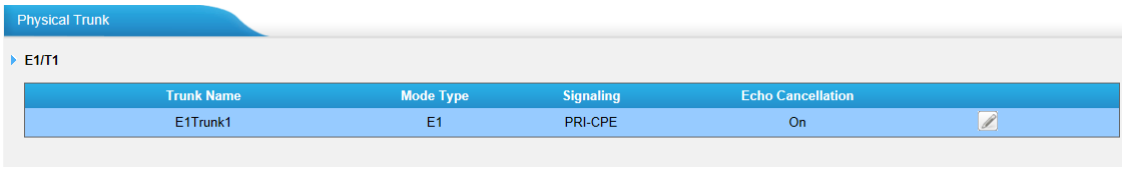



Figure 6-19

On the Physical Trunk page, click 'Edit' on the selected trunk and modify its properties in the popup window:

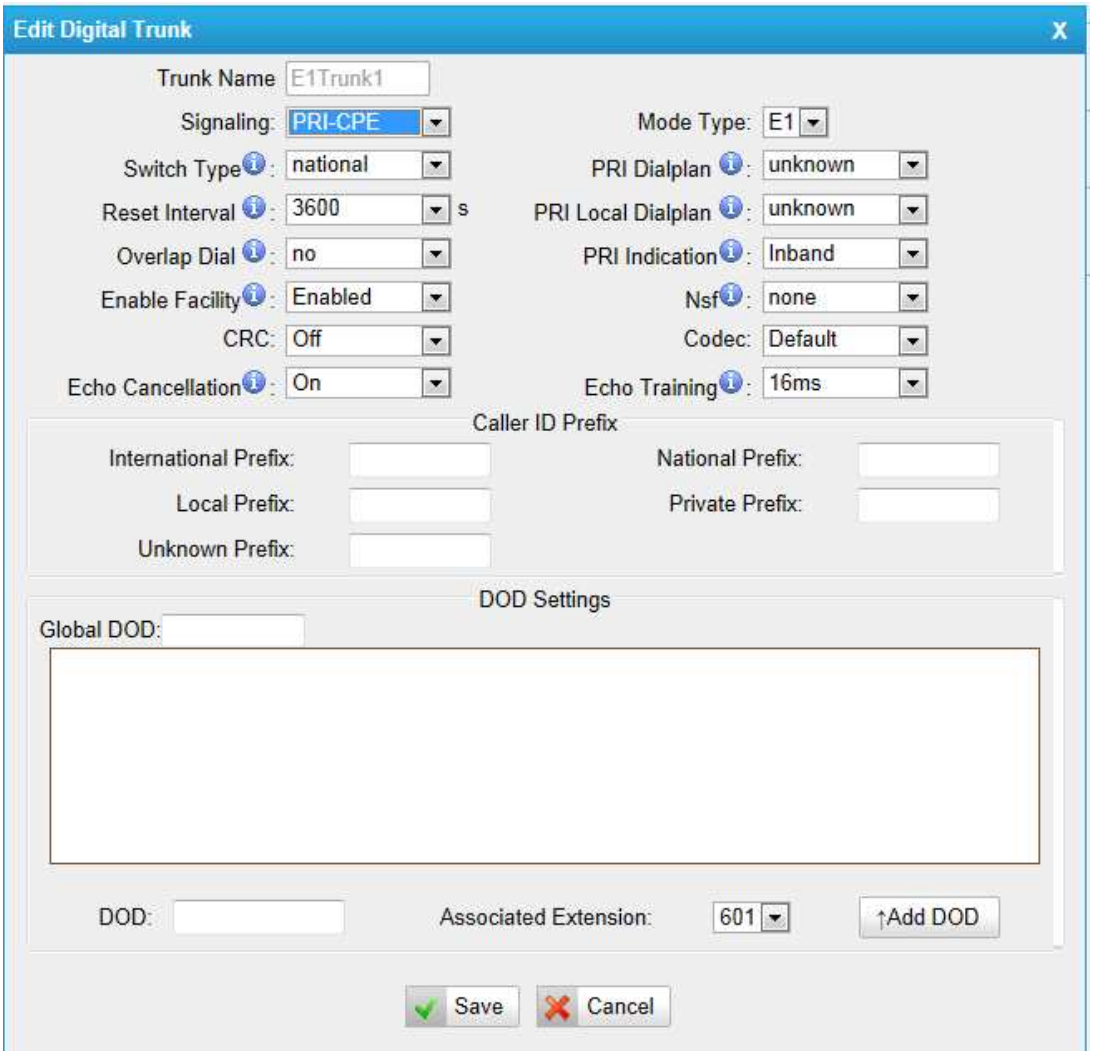



Figure 6-20

**· Trunk name**

Set the trunk name

**·Signaling**
PRI-NET, PRI-CPE,MFC/R2,SS7

**·Mode Type**
E1 / T1 / J1

**·Switch Type**
national: National ISDN type2 (common in the US)
ni1: National ISDN type 1
dms100: Nortel DMS100
4ess: AT&T 4ESS
5ess: Lucent 5ESS
euroisdn: EuroISDN
qsig: Minimalistic protocol to build a "network" with two or more PBX of different vendors!

**·PRI Dial Plan**
Sets an option required for some (rare) switches that require a dial plan parameter to be passed. This option is ignored by most PRI switches. It may be necessary on a few pieces of hardware. This option can almost always be left unchanged from the default.

**·Reset interval**
Sets the time in seconds between restart of unused channels. Some PBXs don't like channel restarts. so set the interval to a very long interval e.g. 100000000 or 'never' to disable *entirely*. If you are in Israel, the following is important: As Bezeq in Israel doesn't like the B-Channel resets happening on the lines, it is best to set the reset interval to 'never' when installing a box in Israel. Our past experience also shows that this parameter may also cause issues on local switches in the UK and China.

**·PRI Local Dial Plan**
Sets an option required for some (rare) switches that require a dial plan parameter to be passed. This option is ignored by most BRI switches. It may be necessary on a few pieces of hardware. This option can almost always be left unchanged from the default.

**·Over Lap Dial**
Define whether mPBX can dial this switch using overlap digits. If you need Direct Dial-in (DDI; in German "Durchwahl") you should change this to yes, then mPBX will wait after the last digit it receives.

**·PRI Indication**

Tells how Device should indicate Busy() and Congestion() to the switch/user. Accepted values are:

inband: Device plays indication tones without answering; not available on all PRI/BRI subscription lines .

outofband: Device disconnects with busy/congestion information code so the switch will play the indication tones to the caller. Busy() will now do same as setting PRI_CAUSE=17 and Hangup().

**·Facility Enable**

To enable transmission of facility-based ISDN supplementary services (such as caller name from CPE over facility).

**·NSF**

Used with AT&T PRIs.If outbound calls are being rejected due to "Mandatory information element missing" and the missing IE is 0x20, then you need this setting.

**·CRC**

CRC Verification.

**·Codec**

Default ,A-Law,U-Law.

**·Echo Cancellation**

Echo cancel Obviously this disables or enables echo cancellation, it is recommended to not turn this off.

**1) CallerID Prefix**

**·International Prefix**

When there are international calls coming in via this BRI trunk, the International Prefix you have set here will be added before the CID. So you can know this is an international call before you answer it.

**·National Prefix**

When there are national calls coming in via this BRI trunk, the National Prefix you have set here will be added before the CID. So you can know this is a national call before you answer it.

**·Local Prefix**

When there are Local calls coming in via this BRI trunk, the Local Prefix you have set here will be added before the CID. So you can know this is a local call before you answer it.

**·Private Prefix**
When there are Private calls coming in via this BRI trunk, the Private Prefix you have set here will be added before the CID. So you can know this is a Private call before you answer it.

**·Unknown Prefix**
When there are calls with unknown number coming via this BRI trunk, the Unknown Prefix you set here will be shown as the caller ID.

**2) DOD Setting**
DOD (Direct Outward Dialing) means the caller ID displayed when dialing out, before configure this, please make sure the provider supports this feature

**·Global DOD**
Global direct outward dialing number.

**·DOD**
Direct Outward Dialing Number.

**·Associated Extension**
The extension make call out via BRI Trunk will display the associated DOD.

## 6.2.2 VoIP Trunk

There are two types of VOIP trunk in mPBX: SIP and IAX, in this page, we can also configure the 'service provider' trunk, which doesn't need the use name and password for authorization, when you have bought a trunk from provide with IP address only, please choose 'service provider' trunk .

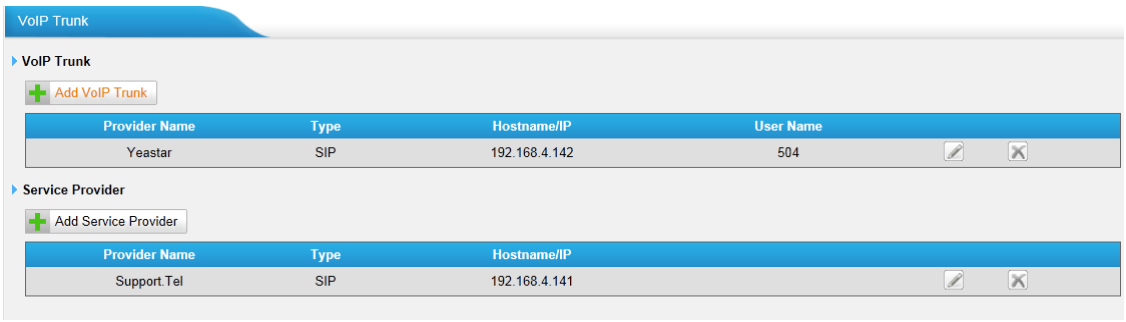



Figure 6-21

### 6.2.2.1 VoIP Trunk

In this page, we can configure VoIP trunk (SIP/ IAX) you have got from provider with the authorization name and password .

**1) Add SIP Trunk**

Input correct SIP information (provide by VoIP provider). Inaccurate

information will prevent the trunk from registering.

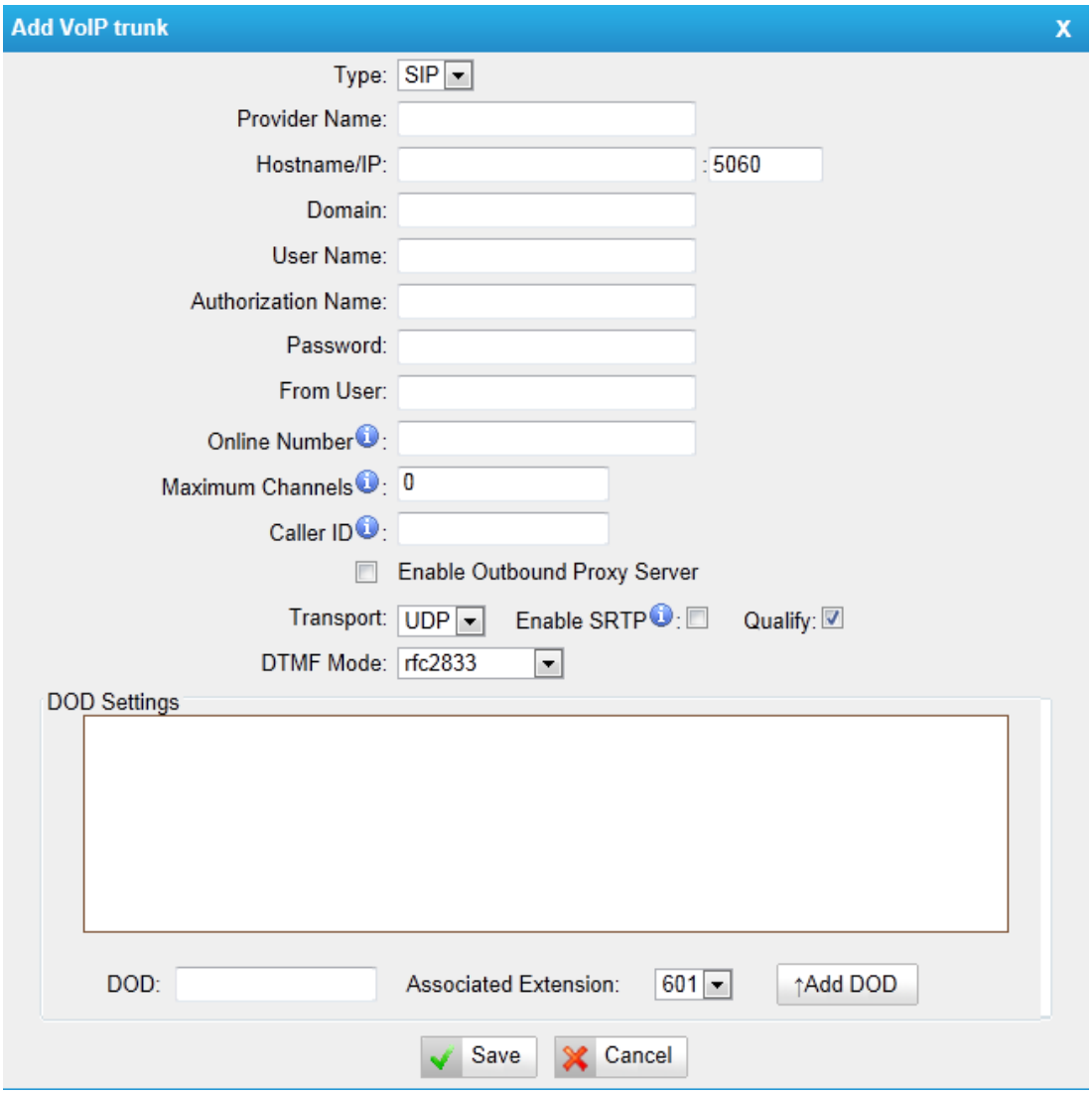



Figure 6-22

**·Type**

SIP – Identifies whether the trunk sends and receives calls using the VoIP protocol SIP

**·Provider Name**

A unique label to help you identify this trunk when listed in outbound rules, incoming rules etc. Ex: 'yeastar'.

**·Hostname/IP**

Service provider's hostname or IP address.5060 is the standard port number used by SIP protocol. Don't change this part if it is not required.

**.Domain**

VoIP provider's server domain name .

**·Username**
Username of SIP account. Used for SIP trunk registration.

**.Authorization name**
Used for SIP authentication. Leave this blank if not required.

**·Password**
Password of SIP account .

**.From User**
All outgoing calls from this SIP Trunk will use the From User (In this case the account name for SIP Registration) in From Header of the SIP Invite package. Keep this field blank if not needed

**.Online number**
Define the online number that expected by 'Skype Connect' and some other SIP service providers. Leave this field blank if not needed.

**·Maximum Channels**
Controls the maximum number of outbound channels (simultaneous calls) that can be used on this trunk . Inbound calls are not counted against the maximum. Set as 0 to specify no maximum.

**·Caller ID**
Specify the caller ID to use when making outbound calls over this trunk. The caller ID set in the 'extension' screen will override the caller ID set in the 'VOIP trunk' screen. Please note that not all the service providers support this feature. Contact your service provider for more information.

**·Outbound Proxy Server**
A proxy that receives requests from a client, even though it may not be the server resolved by the Request-URI.

**·Codecs**
Define the codec for this sip trunk and its priority
**Note**: To change the codec type and priority of this trunk, please create it first, it will appear when you edit it again.

**·Transport**
This will be the transport method used by the SIP Trunk. This method is given by the SIP trunk provider. The options are UDP (default) or TCP or TLS.

**·Enable SRTP**
Define if SRTP is enabled for this trunk

**·Qualify**
Send check alive packets to the sip provider.

**·DTMF mode**
Set default mode for sending DTMF of this trunk. Default setting: rfc2833

**·DOD**
DOD (Direct Outward Dialing) means the caller ID displayed when dialing out, before configure this, please make sure the provider supports this feature

**·Associated Extension**
The extension make call out via SIP Trunk will display the associated DOD

2) Add IAX trunk
Input correct IAX information (provided by VOIP provider). Inaccurate information will prevent the trunk from registering.

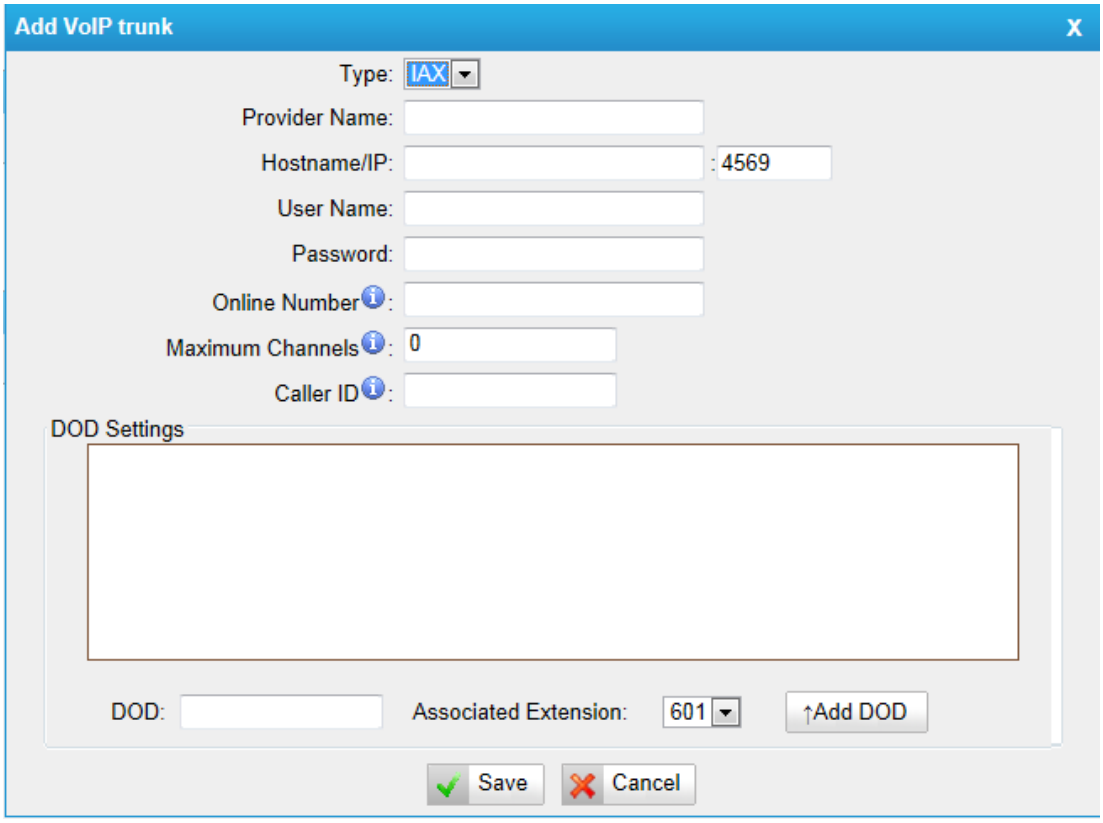



Figure 6-23

**·Type**
IAX – Identifies whether the trunk sends and receives calls by using the VoIP protocol IAX.

**·Provider Name**
A unique label to help you identify this trunk when listed in outbound rules,

incoming rules etc. Ex: 'yeastar2'.

**·Hostname/IP**
Service provider's hostname or IP address. 4569 is the standard port number used by IAX protocol. Don't change this part if it is not required.

**·Username**
Username of IAX account. Used for IAX trunk registration.

**·Password**
Password of IAX account .

**.Online number**
Define the online number that expected by 'Skype Connect' and some other SIP service providers. Leave this field blank if it's no required.

**·Maximum Channels**
Controls the maximum number of outbound channels (simultaneous calls) that can be used on this trunk . Inbound calls are not counted against the maximum. Set as 0 to specify no maximum.

**·Caller ID**
Specify the caller ID to use when making outbound calls over this trunk. The caller ID set in the 'extension' screen will override the caller ID setting in the 'VOIP trunk' screen. Please note that not all the service providers support this feature. Contact your service provider for more information.

**·DOD**
DOD (Direct Outward Dialing) means the caller ID displayed when dialing out, before configure this, please make sure the provider supports this feature

**·Associated Extension**
The extension make call out via IAX Trunk will display the associated DOD

### 6.2.2.2 Service Provider

This is service provider trunk (peer to peer mode), which authorized using IP address only. If you have got a trunk with IP address only, please choose this type

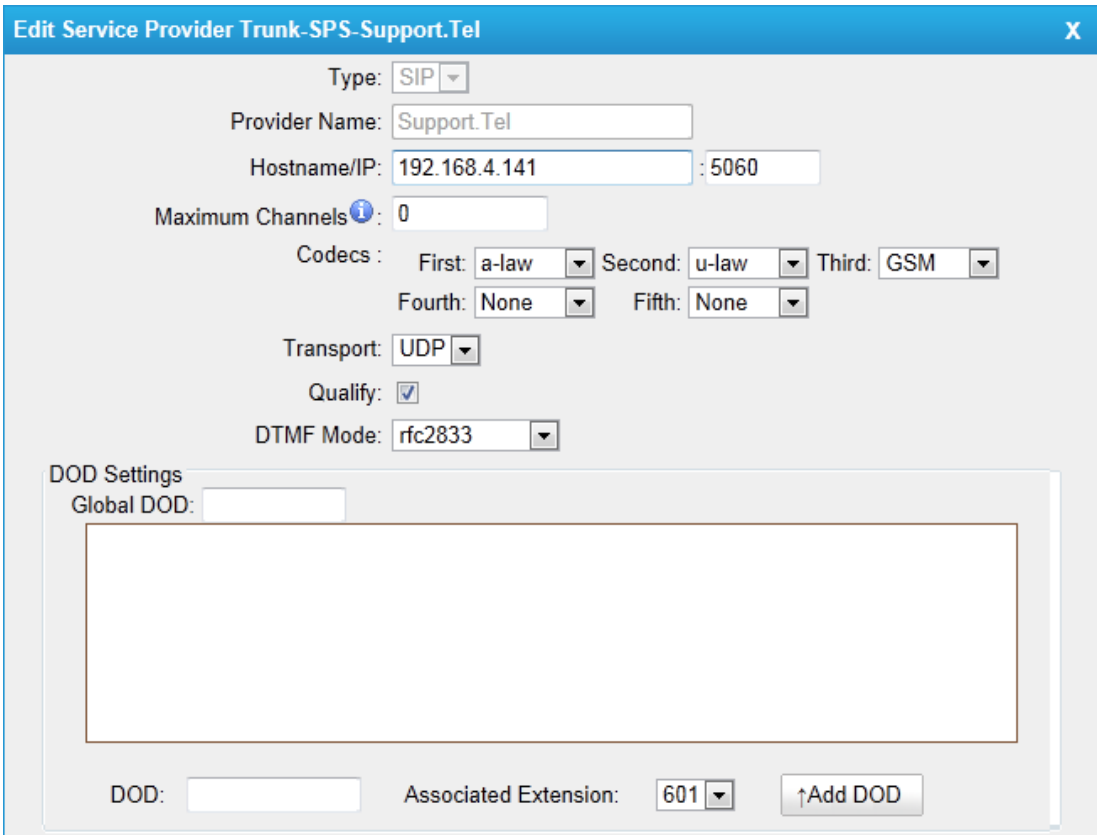



Figure 6-24

**·Type**

SIP or IAX

SIP – Identifies whether the trunk sends and receives calls by using the VoIP protocol SIP.

IAX - Identifies whether the trunk sends and receives calls by using the VoIP protocol IAX.

**·Provider Name**

A unique label would help to you identify this trunk. Ex: 'Provider2'.

**·Hostname/IP**

Service provider's hostname or IP address.

**Note**: 5060 is the standard port number used by SIP protocol, 4569is the standard port number used by IAX protocol. Don't change this part if it is not required.

**·Maximum Channels**

Controls the maximum number of outbound channels (simultaneous calls) that can be used on this trunk. Inbound calls are not counted against the maximum. Leave blank to specify no maximum.

**·Codecs**

Define the codec for this sip trunk and its priority

**Note**: codec can only display when edit it after creating the trunk.

**·Transport**
This will be the transport method used by the SIP Trunk. This method is given by the SIP trunk provider. The options are UDP (default) or TCP or TLS.

**·Qualify**
Send check alive packets to the sip provider.

**·DTMF mode**
Set default mode for sending DTMF of this trunk. Default setting: rfc2833

**·DOD**
DOD (Direct Outward Dialing) means the caller ID displayed when dialing out, before configure this, please make sure the provider supports this feature

**·Associated Extension**
The extension make call out via this Trunk will display the associated DOD.

# 6.3 Outbound Call Control

## 6.3.1 Outbound Routes

In this page, we can configure the outbound rules to control the outgoing calls.
**Note:**
1. The max number of outbound route is 64
2. If the dial patterns are the same in several routes, mPBX will choose the available routes from top to the last one.
3. When you have created a new extension, please edit the outbound route so that he can dial out too

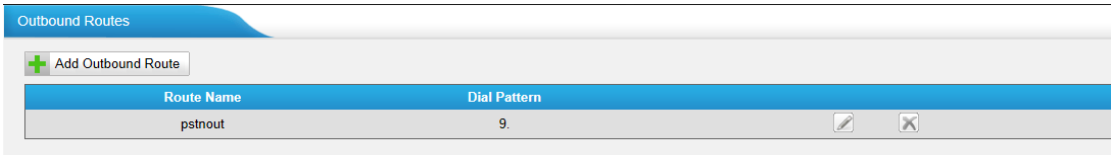



Figure 6-25

We can create outbound route or use the default route 'pstnout' ( dial 9+numbers to dial out)

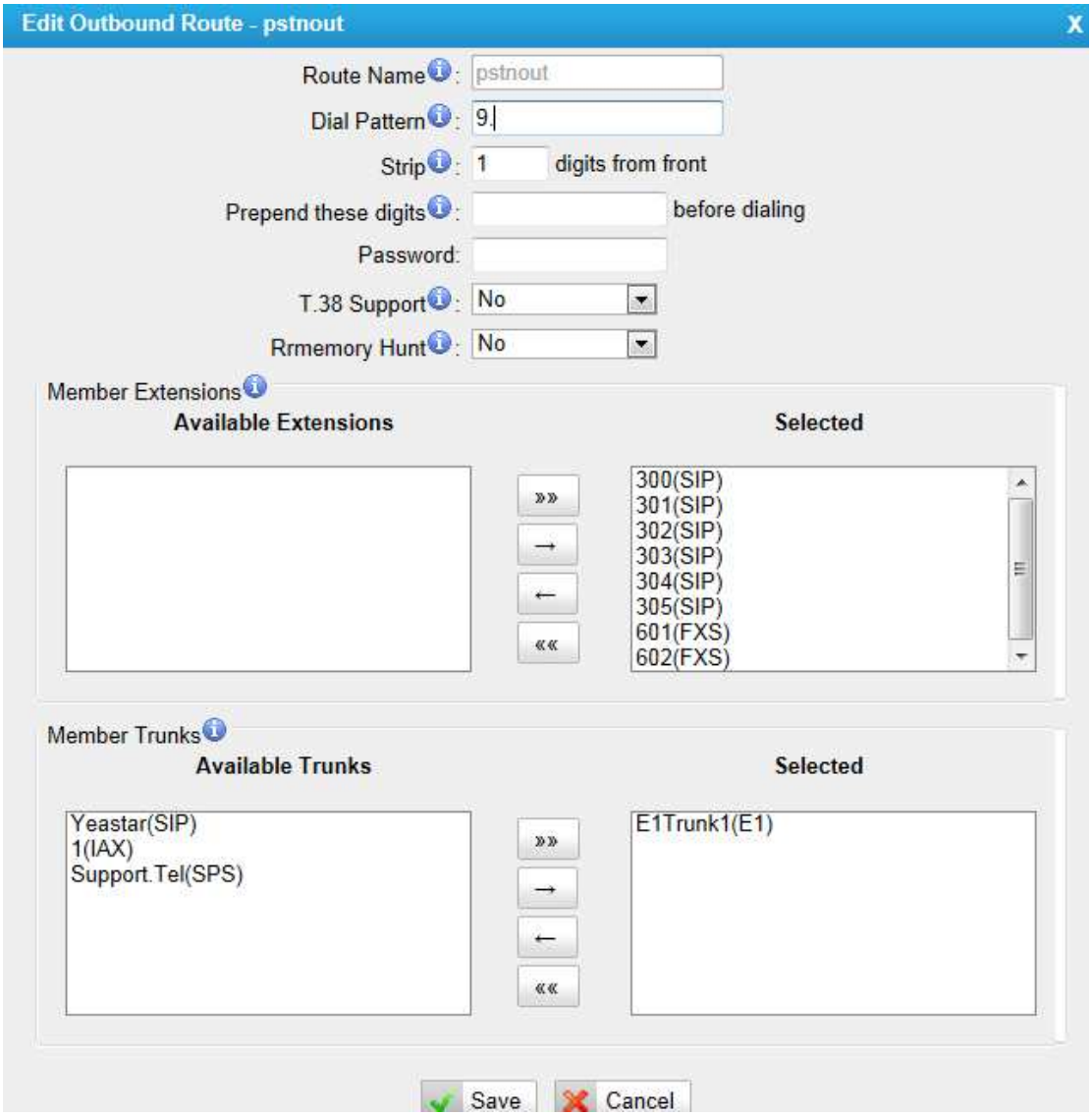



Figure 6-26

**·Route Name**

Name of this Outbound Route. Ex: 'Local' or 'Long Distance' etc.

**·Dial Pattern**

Outbound calls that match this dial pattern will use this outbound route. There are a number of dial pattern characters that have special meanings:

**X**: Any Digit from 0-9

**Z**: Any Digit from 1-9

**N**: Any Digit from 2-9

**[12345-9]**: Any digit in the brackets (in this example, 1, 2, 3, 4, 5, 6, 7, 8, 9)

The '**.**' Character will match any remaining digits. For example, 9011. will match any phone number that starts with 9011, excluding 9011 itself.

The '**!**' will match none remaining digits, and causes the matching process to complete as soon as it can be determined that no other matches are possible.

Example 1: **NXXXXXX** will match any 7 digits phone number.

Example 2: **1NXXNXXXXX** will match a phone number starting with a 1, followed by a 3-digit area code, and then 6 digit number.

**·Strip digits from front**

Allows the user to specify the number of digits that will be stripped from the front of the phone number before the call is placed. For example, if users must press 0 before dialing a phone number, one digit should be stripped from the dial string before the call is placed.

**·Prepend these digits before dialing**

These digits will be prepended to the phone number before the call is placed. For example, if a trunk requires 10 digit dialing, but users are more comfortable with 7 digit dialing, this field could be used to prepend a 3 digit area code to all 7 digit phone numbers before calls are placed.

**·Password**

The route password can be used to protect this route from being accessed without a password.

**·T.38 Support:**

Enable T38 fax in this outbound route(Only for SIP Trunk).

**·Rrmemory Hunt**

Round robin with memory, remembers which trunk was used last time, and then use the next available trunk to call out.

**·Member Extensions**

Defines the extensions that will be permitted to use this outbound route.

**·Member Trunks**

Defines the trunks that can be used for this outbound route.

## 6.3.2Speed Dial Settings

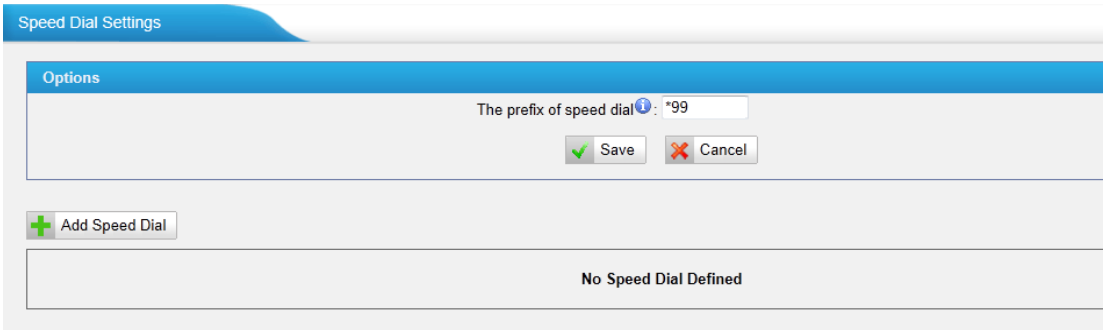



Figure 6-26

1) Options

**·The prefix of speed dial**

The prefix should be dialed before the speed dial number. Default is *99

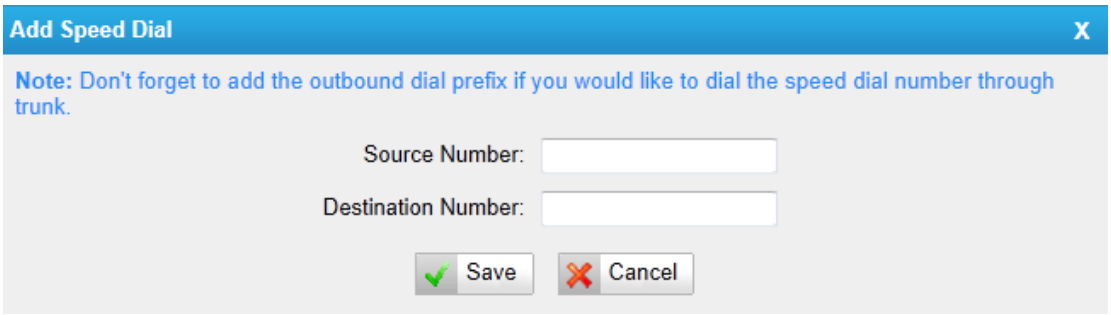

Add Speed Dial
X
Note: Don't forget to add the outbound dial prefix if you would like to dial the speed dial number through trunk.
Source Number:
Destination Number:
Save
Cancel

Figure 6-27

2) Add new speed dial.

**·Source Number**

The speed dial number.

**·Destination Number**

The number you want to call.

e.g. The source number is ”123”. The destination number is 5503305.The prefix number is *99.You can use an extension with any type to dial *99123, then it will call to number 5503305.

**Note:** Don’t forget to add the outbound dial prefix if you would like to dial the speed dial number through trunk.

# 6.4 Inbound Call Control

In this page, we can configure the details of IVR, ring group, queue and inbound routes.

## 6.4.1 IVR

When there’s an inbound call aims at Auto Attendant, mPBX will play an IVR recording and route the caller to the requested destination (for example, ‘Welcome to XX company, for sales press 1, for technical support press 2, for operator press 0, etc’). The system will transfer the call to corresponding extension according to DTMF digits inputted by the user

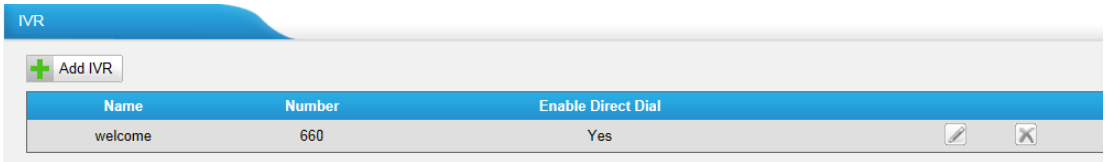



Figure 6-28

There is a default IVR here, we can edit it directly or add IVR by yourself

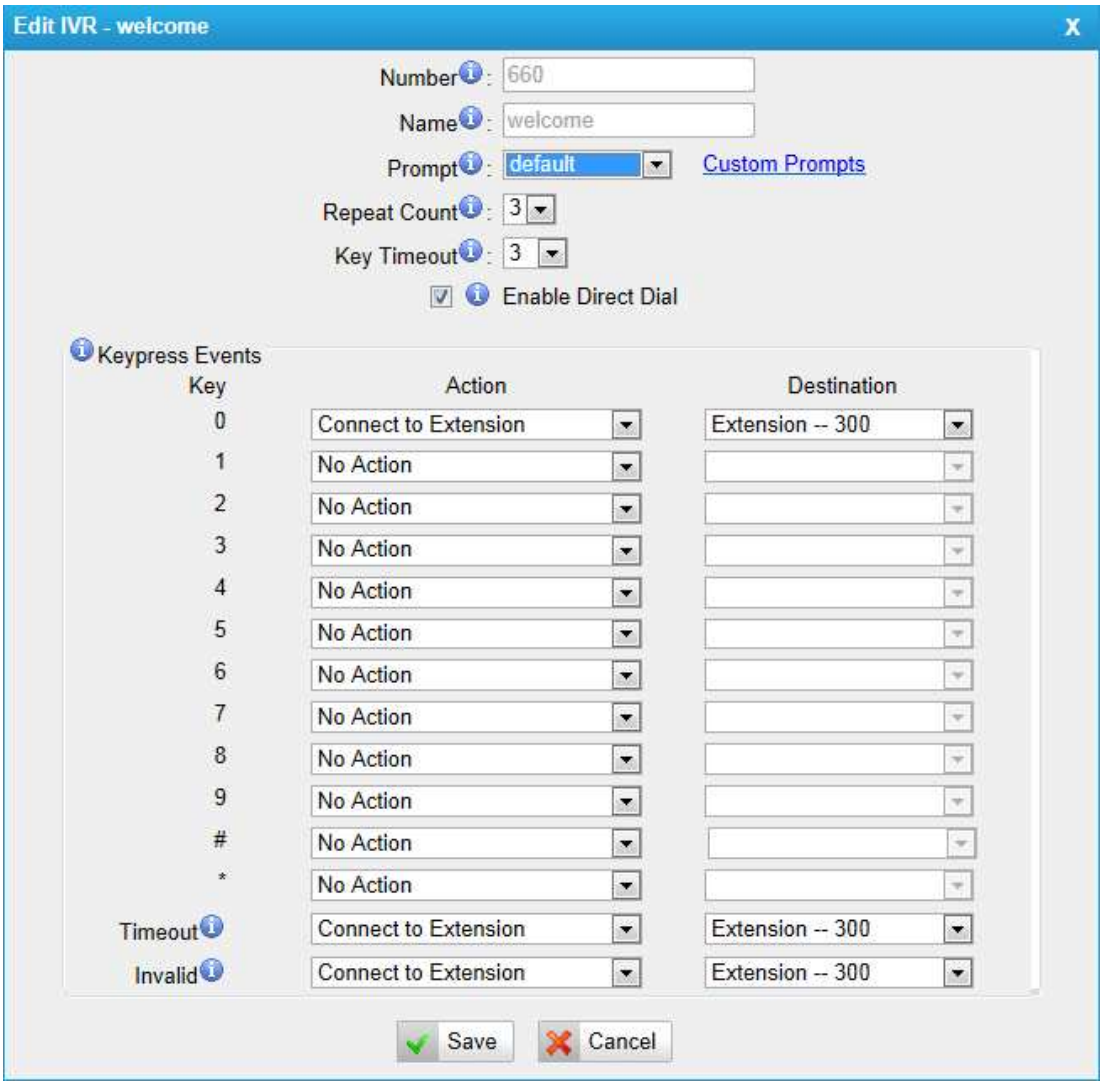



Figure 6-29

**·Number**

mPBX treats IVR as an extension; you can dial this extension number to reach the IVR from internal extension.

**·Name**

A name for the IVR

**·Prompt**

The prompt recording that will be played when this IVR is reached.

**·Repeat Count**

The number of times that the selected IVR prompt will be played.

**·Key Timeout**

Wait for the user to enter a new extension for a specified number of seconds.

**·Enable Direct Dial**

Allow the caller to dial other extensions number directly.

**·Key Press Events**
A list of actions that can be performed depending on the digit dialed by the user.

**·Key**
The Key pressed when the callers hear the IVR prompt.

**·Action**
When the callers press the corresponding key, the action mPBX executes.
No Action: Do nothing
Connect to Extension: Connect the call to an extension.
Connect to Voicemail: Connect the call to the voicemail of an extension
Connect to RingGroup: Connect the call to a ringgroup.
Connect to IVR: Connect the call to an IVR.
Connnect to Conference Room: Connect the call to a conference room.
Connect to DISA: Connect the call to a DISA.
Connect to Queue: Connect the call to a queue.
Connect to Faxes: Connect the call to Faxes of extensions.
Dial by Name:The callers can dial the name of an extension to connect to the corresponding extension.
Hung up: Hung up the call.

**·Destination**
Where will mPBX route the call when the action occurs.

**·Time Out**
Defines the timeout action. A timeout occurs after the IVR prompt has finished playing for the number of times specified by the 'Repeat Count' field.

**·Invalid**
Defines the invalid action. The invalid action is triggered if the user enters a DTMF digit that is not defined for this IVR.

## 6.4.2 Ring Groups

Ring groups can be configured to balance the call traffic for multiple users and give callers a higher level of availability for incoming calls. Multiple ring methods and voicemail are supported.

**Note**: follow me feature in extension page will not take effect when it's ringing as an agent

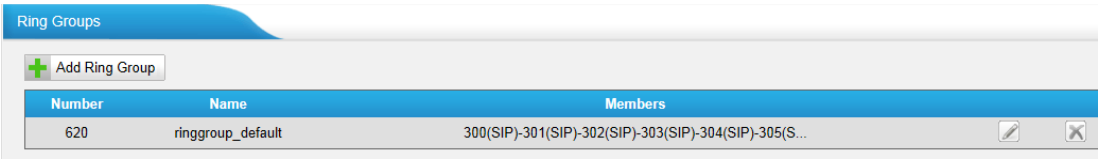



Figure 6-30

There is a default ringgroup, you can edit it or create a new one

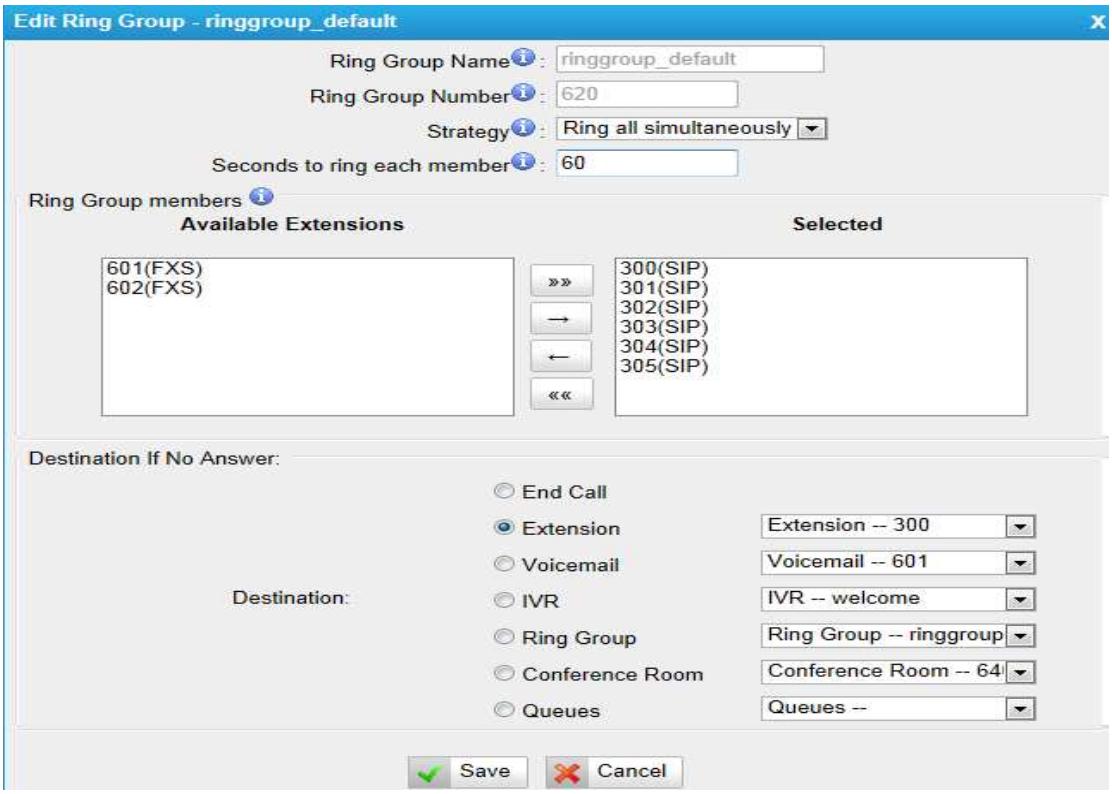



Figure 6-31

**·Ring Group Name**

This option defines a name for this group, i.e. 'Sales'. 'Ring Group Name' is a label to help you identify this group in the group list.

**·Ring Group Number**

This option defines the numbered extension that can be dialed to reach this group.

**·Strategy**

This option sets the Ringing Strategy for this Group. The options are as follows:

1. RingAll Simultaneously: Ring all available Extensions simultaneously.
2. Ring Sequentially: Ring each extension in the group one at a time.

**·Seconds to ring each member**

1. If the strategy is 'Ring All Simultaneously', it means set the number of seconds to ring this group before routing the call according to the 'Destination if No Answer' settings.
2. If the strategy is 'Ring Sequentially', it means set the number of seconds to ring a single extension before moving onto the next one.

**· Ring Group Members**

An extension can be made a member of this ring group by moving it into the 'Selected' box.

**·Destination If No Answer**

When all members on this group fail to answer the call, system will handle the call according to the selected destination.

## 6.4.3 Queues

Call Queues give users (i.e. call centers) an efficient means to have their calls answered in the order they were received to deliver top tier customer service.

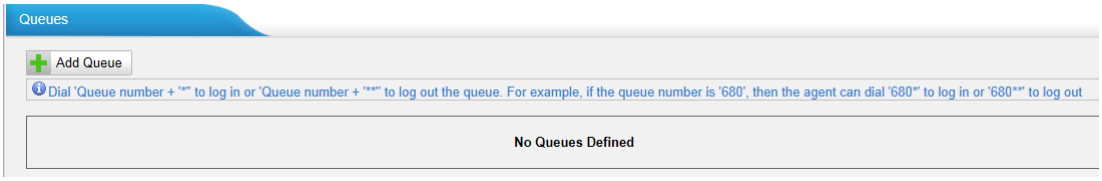

Queues
Add Queue
Dial 'Queue number + '*'' to log in or 'Queue number + '**'' to log out the queue. For example, if the queue number is '680', then the agent can dial '680*' to log in or '680**' to log out
No Queues Defined

Figure 6-32

Call queues allow calls to be sequenced to one or more agents.

**Note**:

1. Dial 'Queue number + '*'' to log in or 'Queue number + '**'' to log out the queue. For example, if the queue number is '680', then agent can dial '680*' to log in or '680**' to log out.
2. Follow me feature in extension page will not take effect when it's ringing as an agent of queue

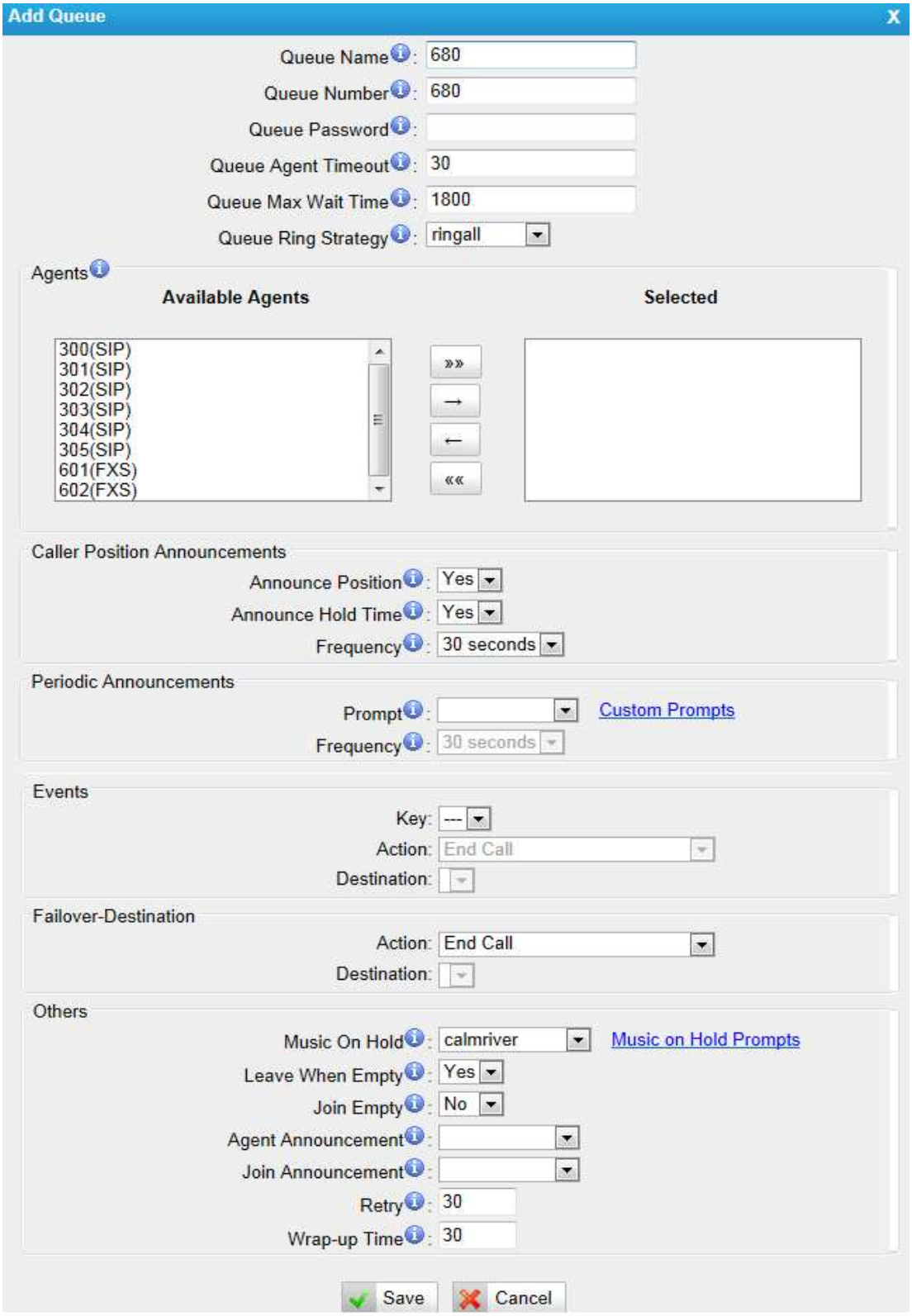



Figure 6-33

**·Queue Name**

A name for the Queue.

**·Queue Number**

Use this number to dial into the queue, or transfer callers to this number to put them into the queue.

**·Queue Password**

You can require agents to enter a password before they can login to this queue. This field allowed to be blank empty, it means the agents can login to this queue without password.

**·Queue Agent Timeout**

The number of seconds an agent's phone can ring before we consider it a timeout.

**·Queue Max Wait Time**

The maximum number of seconds a caller can wait in a queue before being pulled out. (0 for unlimited).

**·Queue Ring Strategy**

This option sets the Ringing Strategy for this Queue. The options are
RingAll: Ring All available Agents simultaneously until one answers.
LeastRecent: Ring the Agent which was least recently called.
FewestCalls: Ring the Agent with the fewest completed calls.
Random: Ring a Random Agent.
RRmemory: Round Robin with Memory, Remembers where it left off in the last ring pass".

1) Agents

This selection shows all users. Selecting a user here makes them a agent of the current queue.

2) Caller Position Announcements

**·Announce Position**

Announce position of caller in the queue

**·Announce Hold Time**

Enabling this option causes mPBX to announce the hold time to the caller periodically based on the frequency timer. Either yes or no; hold time will not be announced if <1 minute.

**·Frequency**

How often to announce queue position and estimated hold time.
**Note**: '0 seconds' means disable the announcement

3) Periodic Announcements

**·Prompt**

Select a prompt file to play periodically.

**·Frequency**
How often to announce a prompt to the caller.

4) Events
If a caller presses the key while waiting in the queue, this setting selects which action should process the key press.

5) Failover-Destination
Define the failover action. A failover occurs after the user reach the Queue max wait time.

6) Others
**·Music On Hold**
Select the 'Music on Hold' Class for this Queue.

**·Leave When Empty**
This option controls whether callers already on hold are forced out of a queue that has no agents. There are two options.
Yes: Callers are forced out of a queue when no agents are logged in.
No: Callers will remain in a queue with no agents.

**·Join Empty**
This option controls whether callers can join a call queue that has no agents. There are two options,
Yes: Callers can join a call queue with no agents or only unavailable agents
No: Callers cannot join a queue with no agents
The default option is No.

**·Agent Announcement**
Announcement played to the Agent prior to bridging in the caller.

**·Join Announcement**
Announcement played to callers once prior to joining the queue.

**·Retry**
The number of seconds we wait before trying all the phones again.

**·Wrap-up time**
How many seconds after the completion of a call an Agent will have before the Queue can ring them with a new call. The default is 30.

## 6.4.4 Conferences

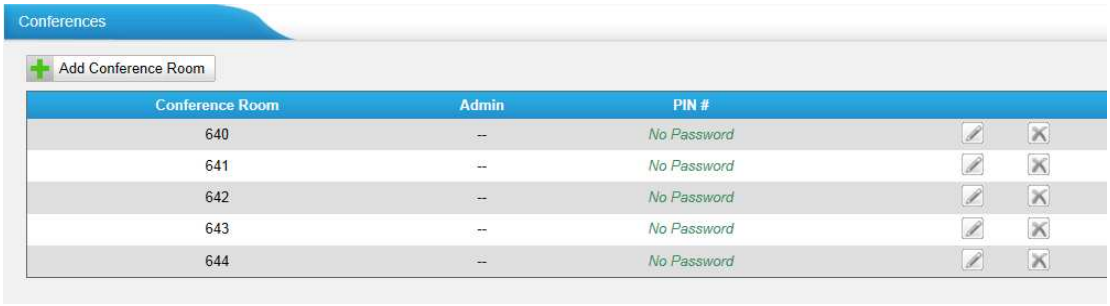



Figure 6-34

Conference Calls increase employee efficiency and productivity, and provide a more cost-effective way to hold meetings. Conference agents can dial * to access to the settings options and the admin can kick the last user out and can lock the conference room.

**·Extension**
This is the number dialed to reach this Conference Room.

**·Admin**
Admin can kick a user out and can lock the conference room.

**·Pin #**
Set a PIN # that must be entered in order to access this conference room (i.e. 1234).

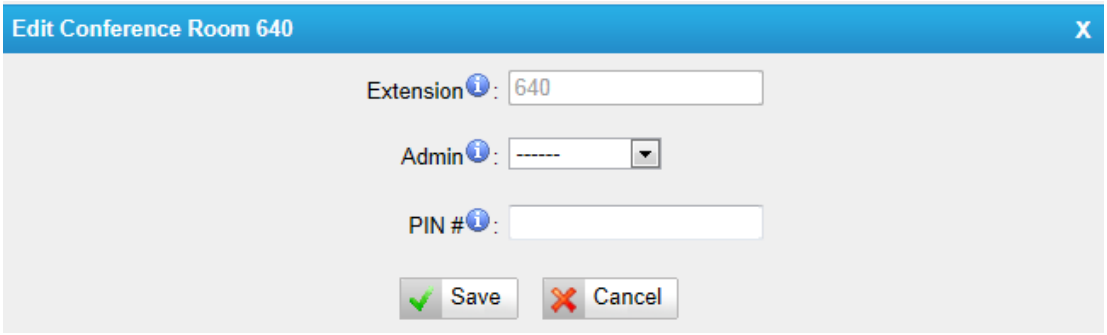



Figure 6-35

## 6.4.5 Inbound Routes

Inbound routing processes incoming call traffic to destination extensions during office hours or outside office hours

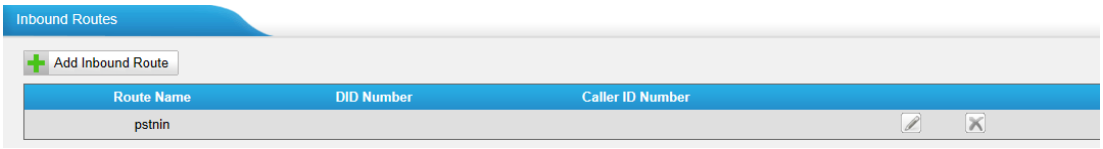



Figure 6-36

There is a default inbound route for all the trunks and set IVR as the destination, you can edit it or create a new one for your demands. When an incoming call arrives, the system will first check 'fax detection', then 'Holidays', at last 'Business Days'.

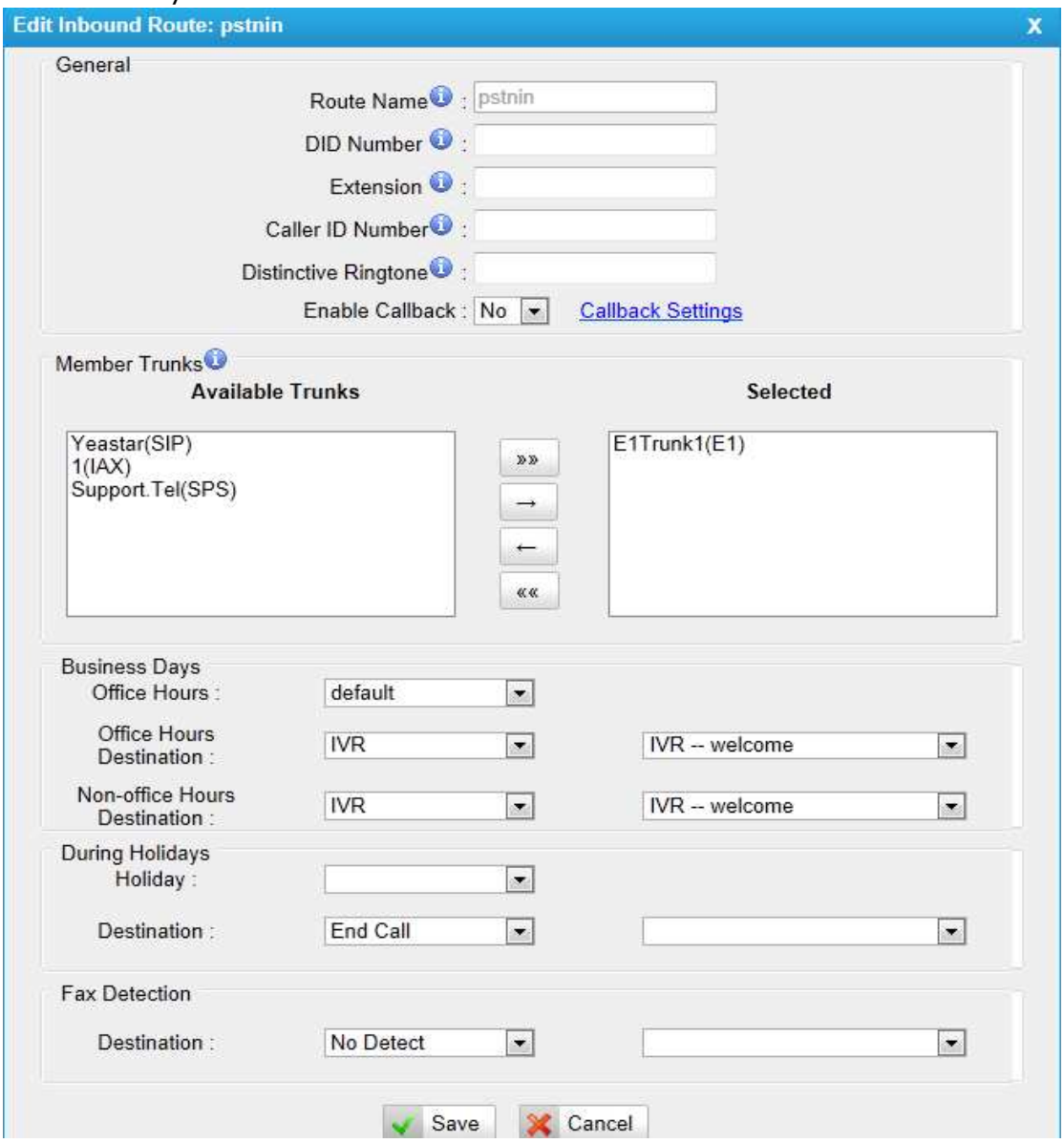



figure 6-37

General

**·Route Name**

A name for this inbound route. Ex: 'pstnin' etc.

**·DID Number**

Define the expected DID Number if this trunk passes DID on incoming calls. Leave this field blank to match calls with any or no DID info. You can also use pattern matching to match a range of numbers. The following patterns may be used:
**X**: Any Digit from 0-9
**Z**: Any Digit from 1-9
**N**: Any Digit from 2-9
**[12345-9]**: Any digit in the brackets (in this example, 1,2,3,4,5,6,7,8,9)
The '**.**'Character will match any remaining digits. For example, 9011. will match any phone number that starts with 9011, excluding 9011 itself.
The '**!**' will match none remaining digits, and causes the matching process to complete as soon as it can be determined that no other matches are possible.

Example 1: **NXXXXXX**will match any 7 digits phone number.
Example 2: **1NXXNXXXXX**will match a phone number starting with a 1, followed by a 3-digit area code, and then 6 digit number.

For more information, please refer to **Appendix G How to Use DID.**

**·Extension**
Define the extension for DID number. This field is only valid when you use BRI, SIP, SPS or SPX trunk for this inbound router. You can only input number and '-'in this field, and the format can be xxx or xxx-xxx. The count of the number must be only one or equal the count of the DID number.

**·Caller ID Number**
Define the Caller ID Number to be matched on incoming calls. Leave this field blank to match any or no DID info.
You can also use a pattern match (e.g. 2[345]X) to match a range of numbers. The following patterns may be used:
**X**: Any Digit from 0-9
**Z**: Any Digit from 1-9
**N**: Any Digit from 2-9
**[12345-9]**: Any digit in the brackets (in this example, 1,2,3,4,5,6,7,8,9)
The '**.**'Character will match any remaining digits. For example, 9011. will match any phone number that starts with 9011, excluding 9011 itself.
The '**!**' will match none remaining digits, and causes the matching process to complete as soon as it can be determined that no other matches are possible.

Example 1: **NXXXXXX**will match any 7 digits phone number.
Example 2: **1NXXNXXXXX**will match a phone number starting with a 1, followed by a 3-digit area code, and then 6 digit number.

**·Distinctive Ringtone**

mPBX support mapping to custom ring tone files. For example, if you configure the distinctive ringing for custom ring tone to '**Family**', the ring tone will be played if the phone receives the incoming call. This feature works with all IP phones which support distinctive ringtone.

How do I configure distinctive ring tones? Please refer to APPENDIX E.
**Note:** If you want to use feature Distinctive ringtone, please confirm you're your IP phone support this feature firstly. Currently distinctive ringtone can be compatible with Yealink and Snom phone.

**·Enable Callback**
You can enable the callback function of this inbound route. If you want to configure the callback function, please refer to **chapter 3.5.12**

Member Trunks
This area allows you to select which trunks will be member trunks for this route. To make a trunk a member of this route, please move it to the 'Selected' box.

Business Days
Define where the calls will be routed during Business Days.

**·Office Hours**
Select one defined business days office hours.

**·Office Hours Destination**
Configure where to route the incoming calls during office hours.

·End Calls
Route the incoming calls to end calls, System will auto hang-up the call.

·Extension
Route the incoming calls to a specific extension.

·Voicemail
Route the incoming calls to extension's voicemail.

·IVR
Route the incoming calls to a specific IVR.

·Ring Group
Route the incoming calls to a specific Ring Group.

·Conference Room
Route the incoming calls to a specific Conference Room.

·DISA
Route the incoming calls to a specific DISA.

·Queues
Route the incoming calls to a specific Queue.

·Faxes
Route the incoming faxes to a specific extension's mail address.
Note: This function only supports T.38 faxes.

·Outbound Routes
Route the incoming calls to a specific outbound route.

This function is mainly used for the connection of two branches.
For example: Company A locates headquarters in the USA with a branch B in China. A and B both have mPBX phone systems.
Now if staff of A would like to make a call to a telephone or mobile phone in China from the extension of A but via the FXS line of B, that can be done by this configuration.

**·Non-office Hours Destination**
Configure where to route the incoming calls during non-office hours.

During Holidays
Define where the calls will be routed during Holidays.

**·Holiday**
Select the defined Holiday to use. When a time is defined in both Business Days and Holidays, it will be treated as Holidays.

**·Destination**
Configure where to route the incoming calls during holidays.

Fax Detection
Configure if detecting faxes in this inbound route.

**Note:** Please choose IVR as the destination above before configure fax detection (recommend)

**·Destination**
Configure where the faxes will be routed when faxes are detected.

**·No detect**
Do not detect faxes.

**·Custom Email**

Customize an E-mail address to receive the faxes. You should first configure the 'Voicemail Settings->SMTP Settings for Voicemail' correctly before you use this option.

**·Faxes**

Send faxes to an extension. If choosing a FXS extension here, the fax will be sent to the FXS port selected, you should connect a fax machine to this FXS port. If Choosing a VoIP extension, the fax will be sent to the extension's voicemail as an attachment.

**Note**: If you receive faxes with custom Email address, the 'SMTP settings' of 'Voicemail Settings' should be configured successfully in advance. If you receive faxes with E-mail address configured in VOIP extension voicemail, you should first make sure the tested email to your email address works fine.

# 6.5 Audio Settings

It's allowed to customize the prompts in mPBX, including the Audio In and change the system prompts to your local country.

## 6.5.1 Custom Prompts

We can record or upload the prompts in this page, you can also play it directly to confirm if it's a valid one, you can also download it and save it as an backup

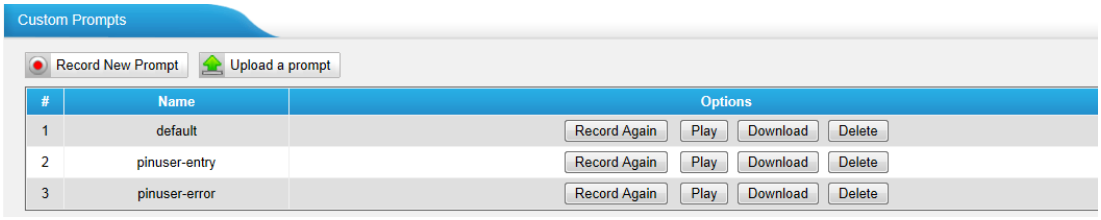

Custom Prompts
Record New Prompt
Upload a prompt
# Name Options
1 default Record Again Play Download Delete
2 pinuser-entry Record Again Play Download Delete
3 pinuser-error Record Again Play Download Delete

Figure 6-38

**1. Record new Prompt**

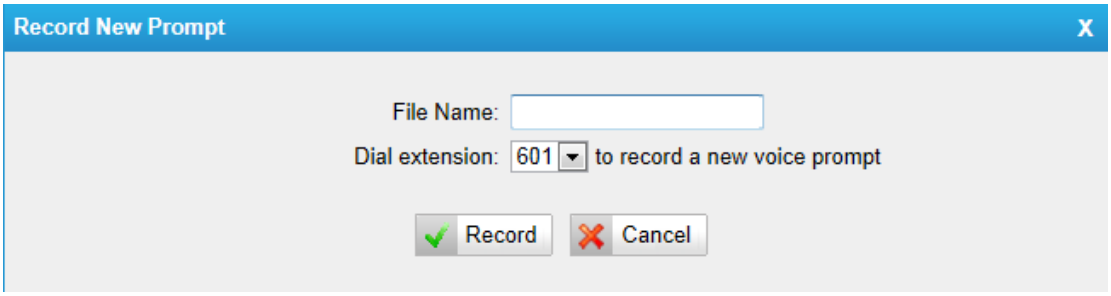



Figure 6-39

The administrator can use this screen to record custom prompts by doing the following:

1）Click 'Record New Custom Prompt'

2) Input the desired file name on the popup window and choose an extension to call for recording (such as 500).

3) Click 'Record'. The selected extension will ring and you can pick up the phone to start recording.

**2. Upload Prompt**

Figure 6-40

The administrator can also upload prompts by doing the following:

1)）Click 'Upload Prompt'.

2) Click 'Browse' to choose the desired prompt.

3) Click 'Upload' to upload the selected prompt.

**Note**: The file size must not be larger than 1.8MB, and the file must be WAV format:

GSM 6.10 8kHz, Mono, 1Kb/s;

Alaw/Ulaw 8kHz, Mono, 1Kb/s;

PCM 8kHz, Mono, 16Kb/s.

## 6.5.2 Music on Hold Prompts

In this page, we can upload the music on hold prompts or adjust the volume from Audio In interface (Only available in WELL mPBX-U110R)

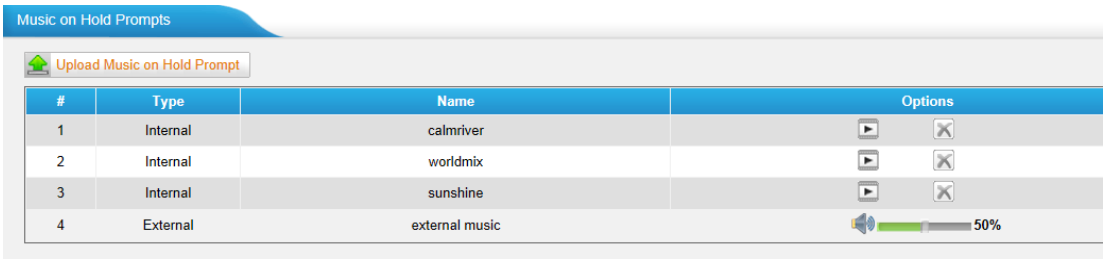



Figure 6-41

The administrator can upload on hold music as follows:

1) Click 'Upload Music on Prompt '

2) Click 'Browse' to choose the desired audio file.

3) Click 'Upload' to upload the selected file.

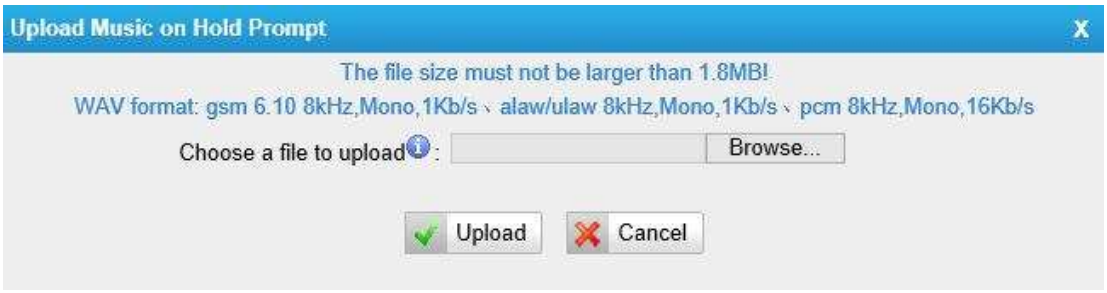

Upload Music on Hold Prompt
The file size must not be larger than 1.8MB!
WAV format: gsm 6.10 8kHz,Mono,1Kb/s、alaw/ulaw 8kHz,Mono,1Kb/s、pcm 8kHz,Mono,16Kb/s
Choose a file to upload:
Browse...
Upload
Cancel

Figure 6-42

**Note**: The sound file format should be as follows:
GSM 6.10, 8.000kHz, Mono, 1kb/sec;
Alaw/Ulaw 8.000kHz, Mono, 1kb/sec;
PCM 8.000kHz, Mono, 16kb/sec.
The file size must not be greater than 1.8MB.

## 6.5.3 System Prompts Settings

mPBX have prompts of many languages. You can download the appropriate language you need. mPBX can support American English, Australian English, Chinese, Dutch, French, Canadian French, German, Greek, Hungarian, Italian, Polish, Portuguese, Brazilian Portuguese, Russian, Spanish, Mexican Spanish, Turkish, Thai, Korean, Danish, Finnish, Norwegian, Swedish, Arabic, British currently.

**Note:**

1. Auto-detection is highly recommended. But if you prefer to download via HTTP or TFTP server, please contact the local dealer for the prompts
2. When update successfully, just click 'apply the changes' on web then it will take effect, there is no need to reboot.

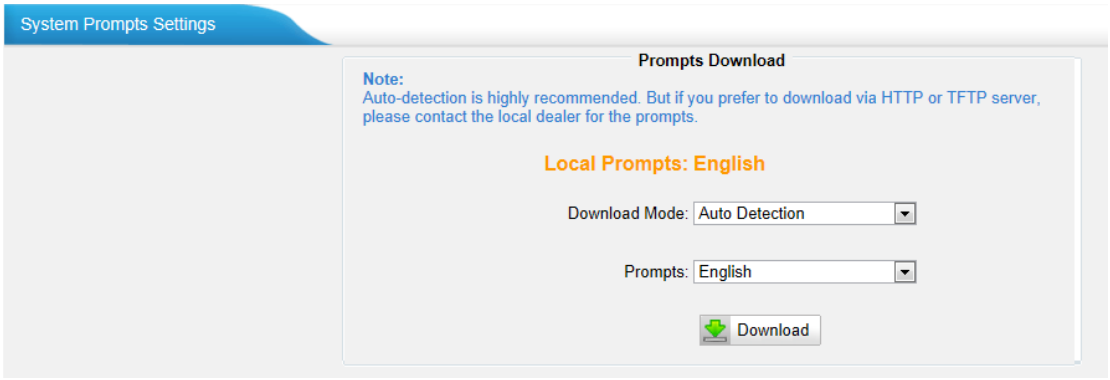

System Prompts Settings
Prompts Download
Note:
Auto-detection is highly recommended. But if you prefer to download via HTTP or TFTP server, please contact the local dealer for the prompts.
Local Prompts: English
Download Mode: Auto Detection
Prompts: English
Download

Figure 6-43

# 6.6 Basic Settings

There are some basic settings we need to configure WELL mPBX-U110R,like the

general preferences, business hours, feature codes, voicemail settings

## 6.6.1 General Preferences

In this page, there are some general settings of mPBX

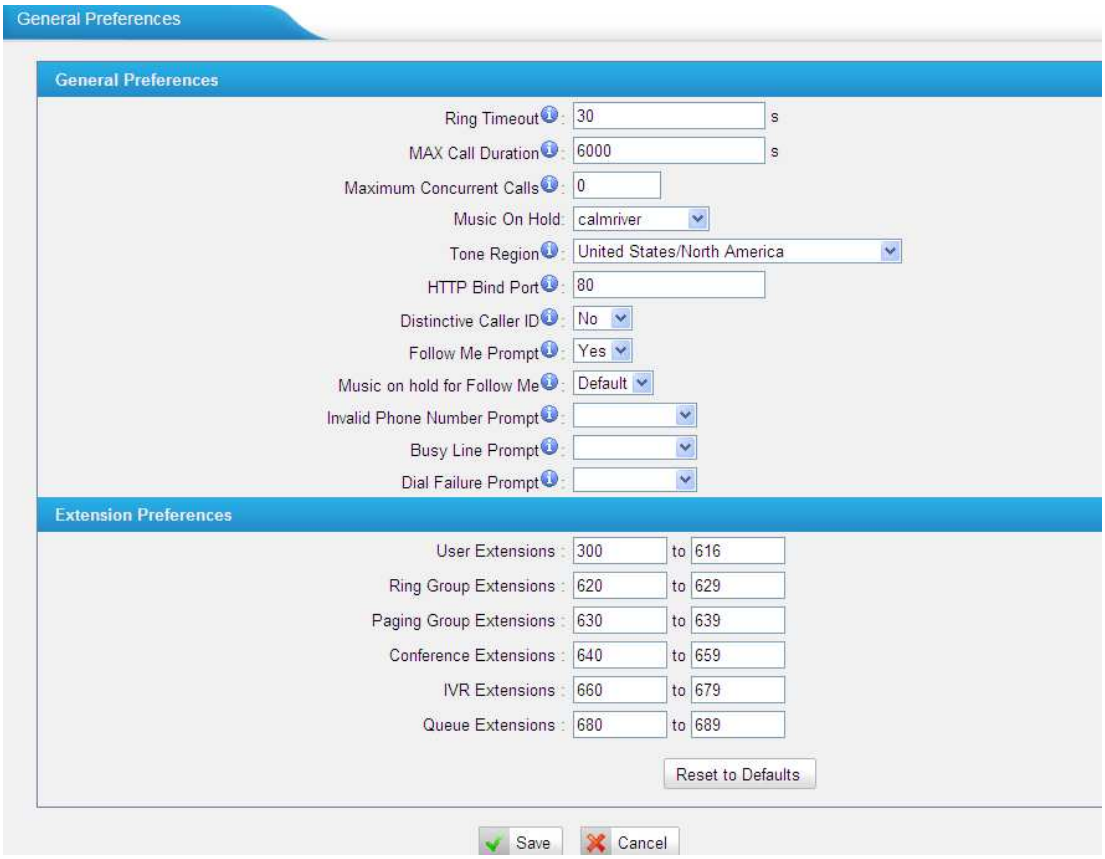

General Preferences
General Preferences
Ring Timeout : 30 s
MAX Call Duration : 6000 s
Maximum Concurrent Calls : 0
Music On Hold : calmriver
Tone Region : United States/North America
HTTP Bind Port : 80
Distinctive Caller ID : No
Follow Me Prompt : Yes
Music on hold for Follow Me : Default
Invalid Phone Number Prompt :
Busy Line Prompt :
Dial Failure Prompt :
Extension Preferences
User Extensions : 300 to 616
Ring Group Extensions : 620 to 629
Paging Group Extensions : 630 to 639
Conference Extensions : 640 to 659
IVR Extensions : 660 to 679
Queue Extensions : 680 to 689
Reset to Defaults
Save
Cancel

Figure 6-44

1) General

**·Ring Timeout**

Number of seconds to ring a device before handling the call as per the extension's Follow Me settings . Default value is 30s.

**.MAX call duration**

The absolute maximum amount of time permitted for a call. A setting of 0 disables the timeout. Default value is 6000s.

**.Maximum concurrent calls**

Maximum concurrent calls limits. Default value 0 means no limit

**·Music on hold**

Used to set hold music for the system.

**Note:** if you need use the 'live music' from 'Audio In' interface, please choose ' external music' here.

**·Tone Region**
Please select your country or nearest neighboring country to enable the default dial tone, busy tone, and ring tone for your region.
**Note**: please reboot the system to take it effect.

**·HTTP bind port/Web Access Port**
Port to use for HTTP sessions. Default: 80
**Note**: please reboot the system to take it effect.

**· Distinctive Caller ID**
When incoming calls are routed from ring group/queue/IVR, the caller ID displays with the name of ring group/queue/IVR , for example 5503302(ringgroup_default)

**Note**: To display IVR's name, please press the key instead of the extension number directly.

**·Follow Me Prompt**
Configure whether to play a prompt 'please wait while trying to look at the person you are calling' when transfer a call by follow me settings.

**·Music on hold for Follow Me**
Choose to play default music-on-hold, ringing tone or stay mute while 'Follow Me'.

**·Invalid Phone Number Prompt**
Configure the prompt when the dialed phone number is invalid.

**·Busy Line Prompt**
Configure the prompt when the dialed phone number is busy.

**·Dial Failure Prompt**
Configure the prompt when dial failed due to conjunction no-available channel.

2) Extension Preferences
**·User Extensions**
The default value is 500 to 616

**·Ring Group Extensions**
The default value is 620 to 629

**·Paging Group Extensions**
The default value is 630 to 639

**·Conference Extensions**
The default value is 640 to 659

**·IVR Extensions**
The default value is 660 to 679

**·Queue Extensions**
The default value is 680 to 689

## 6.6.2 Business Hours

Business hours including 'holiday configuration' is used to control the incoming calls, we can configure it in this page.

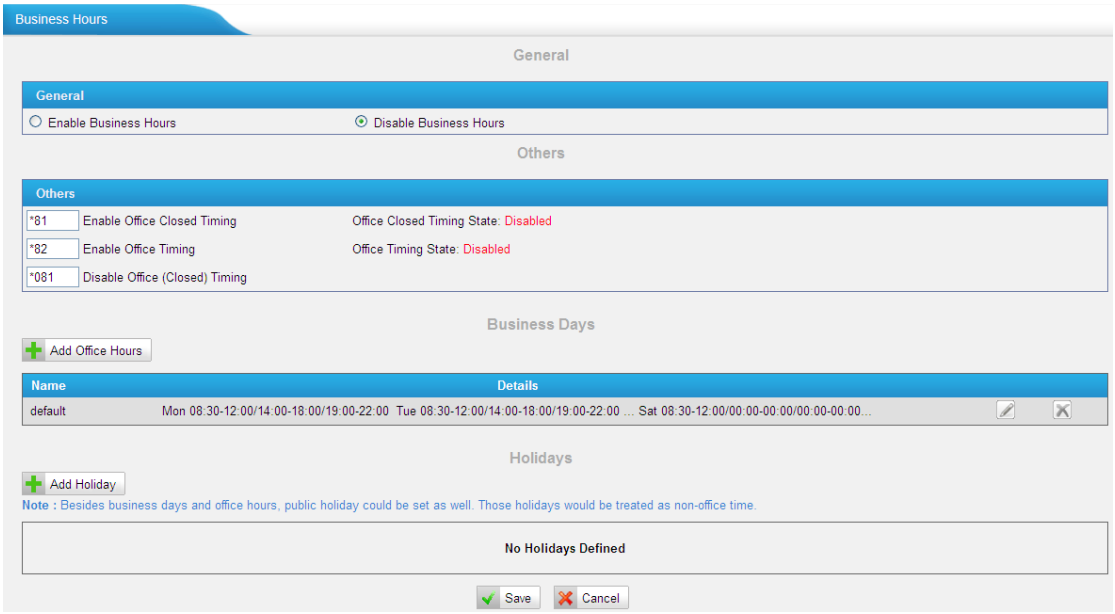



Figure 6-45

1) General
**·Enable Business Hours**
**·disable Business Hours**

2) Others
**·Enable Office Closed Timing**
By dialing *81 (*81 is default) on an extension will force the office time closed for the device whatever the general setting is.

**·Enable Office Timing**
By dialing *82 (*82 is default) on an extension will force the office time enalbed for the device whatever the general setting is.

**·Disable Office closed timing**
By dialing *081 (*081 is default) on an extension will disable the Office Closed

Timing.

3) Add office hours
You can setup the business hours here.

4) Add Holiday
You can setup the holidays here.
If a time period is configured as both Holidays and office hours, it will be treated as Holidays.

## 6.6.3 Feature Codes

There are many feature codes available in mPBX, which allow users to dial from extension side to realize the exact feature

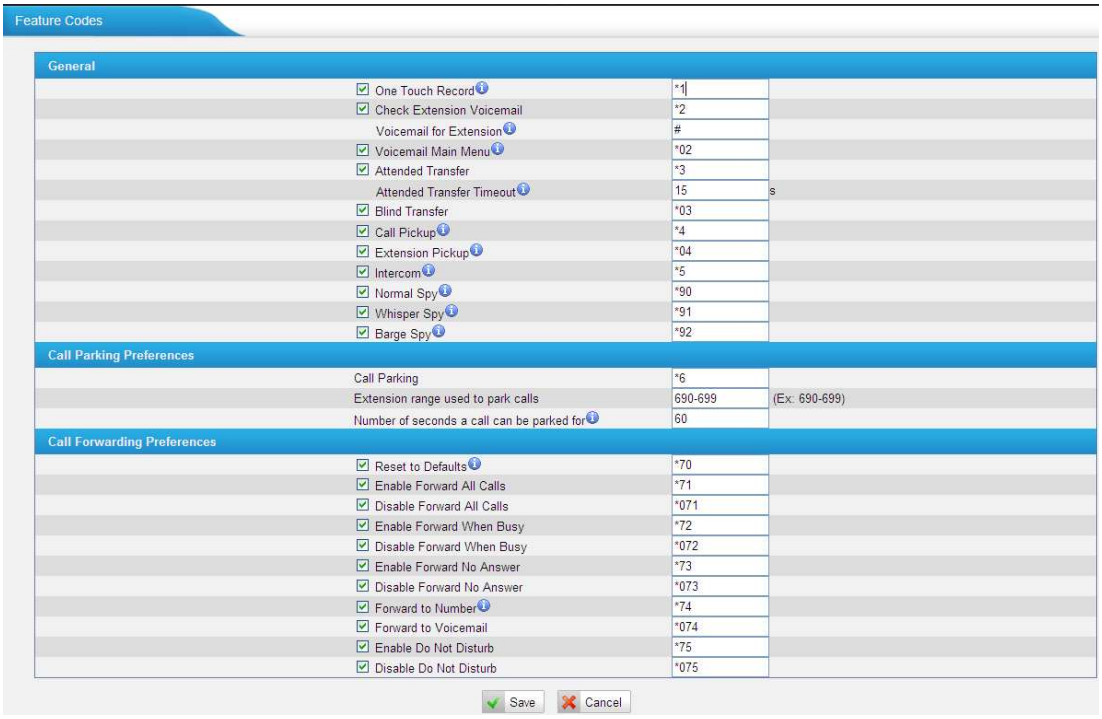



Figure 6-46

1) General

**·One Touch Record**

A user may initiateor stop call recording by dialing *1during a call. (*1 is default setting)

**·Extension for Checking Voicemail**

Users can check their Voicemail by dialing *2 on their phone (*2 is default setting).

**·Voicemail for Extension**

Users can leave a voicemail to other extensions by dialing # on their phone or

the incoming call could be forwarded to an extension's voicemail directly. (# is default setting).

For example, extension 500 want to leave a message for extension 501, users can use 500 dial'#501' to enter the voicemail of 501.

**·Voicemail main menu**
Users can go to the main menu by dialing *02 (*02 is default setting).

**·Attended Transfer**
Users may transfer an incoming call by dialing *3 on their phone (*3 is default setting).

**·Attended Transfer Timeout**
The time out of transferring a call

**·Blind Transfer**
Users may blind transfer an incoming call by dialing*03 on their phone (*03 is default setting).

**·Call Pickup**
Users may pick up an incoming call by dialing *4 on their phone (*4 is default setting)

**·Extension Pickup**
Users may pick up a specific extension's incoming call by dialing *04+extension number on their phone (*04 is default setting)

**·Intercom**
Define the feature code that is used to dial an extension in intercom mode. For instance setting this value to *5 would allow you to initiate an intercom call with extension 501 by dialing *5501.

**·Normal Spy**
In this mode, you can only listen to the extension being spied, for example you can dial *90501 to monitor extension 501

**·Whisper Spy**
In this mode you can listen/whisper to the extension being spied, for example, dialing *91501 to listen to extension 501, you can also talk with 501 too.

**·Barge Spy**
In this mode, you can barge in both extensions involved the call, for example dialing *92501 to barge in and talk with all the extensions inside

2) Call Park Preferences

**·Call Parking**

User may park an incoming call on his own telephone by pressing '*6'(*6 is default setting)

**·Extension range used to park calls**

User may park an incoming call on a designated extension at first and then pick up the call again on any other extension.

**·Number of seconds a call can be parked before it is recalled.**

Defines the number of seconds that a call can be parked before it is recalled to the station that parked it.

3) Call Forwarding Preferences

**·Reset to Defaults**

Users may reset all call forward defaults by calling *70 on their phone (*70 is default setting).

**Note**: When reset to defaults. The call forwarding settings will be configured as follows:
Always forward: Disabled
Busy forward to Voicemail: Enabled
No answer forward to Voicemail: Enabled
Do not disturb: Disabled

**·Enable Forward All Calls**

Users may enable always forward by calling *71 on their phone (*71 is default setting)

**·Disable Forward All Calls**

Users may disable always forward by calling *071 on their phone (*071 is default setting)

**·Enable Forward When Busy**

Users may enable busy forward by dialing *72 on their phone (*72 is default setting)

**·Disable Forward When Busy**

Users may disable busy forward by calling *072 on their phone (*072 is default setting)

**·Enable Forward No Answer**

Users may enable no answer forward by calling *73 on their phone (*73 is default setting)

**·Disable Forward No Answer**
Users may disable no answer forward by calling *073 on their phone (*072 is default setting)

**·Forward to number**
Users may activate call forwarding by dialing this feature code, followed by the extension or phone number to forward all calls to.

**Note**: Users may activate Forward to number by dialing *74 + phone number. e.g.: by dialing *74501, all calls will be forwarded to extension 501.

**·Forward to Voicemail**
Users may forward the call to Voicemail by calling *074 on their phone (*074 is default setting)

**·Enable Do Not Disturb**
Users may enable do not disturb by calling *75 on their phone (*75 is default setting)

**·Disable Do Not Disturb**
Users may disable do not disturb by calling *075 on their phone (*075 is default setting)

## 6.6.4 Voicemail Settings

In this page, we can configure some settings for voicemail feature, including general voicemail settings and SMTP settings, which is used for 'voicemail to email'

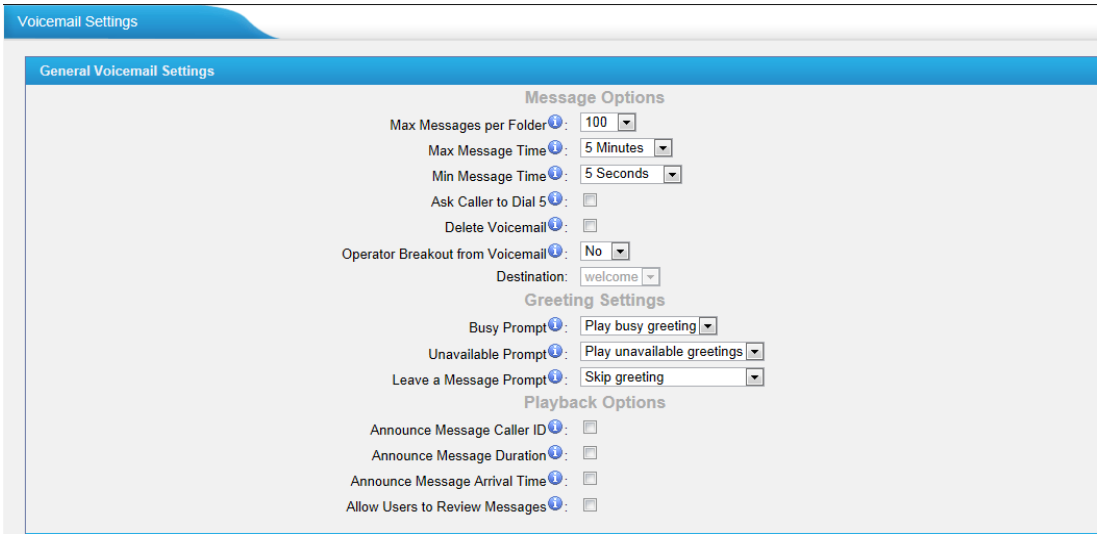



Figure 6-47

1) General Voicemail Settings

a) Message Options

**·Max Messages per Folder**

Set the maximum number of messages that can be stored in a single voicemail box.

**·Max Message Time**

Set the maximum length of a single voicemail message.

**·Min Message Time**

Set the minimum length of a single voicemail message. Messages below this threshold will be automatically deleted.

**·Ask Caller to Dial 5**

If this option is set, the caller will be prompted to press 5 before leaving a message.

**·Operator Breakout from Voicemail**

If this option is set, the caller can jump out of the voicemail and go to the destination (IVR) you set by dialing "0".

b) Greeting Settings

**·Busy Prompt**

Greeting played when the extension called is busy.
Skip greeting: Do not play a greeting.
Play busy greeting: play the extension busy greeting.

**·Unavailable Prompt**

Greeting played when the extension called is Unavailable.
Skip greeting: Do not play a greeting.
Play Unavailable greeting: play the extension Unavailable greeting.

**·Leave a Message Prompt**

Greeting played to ask the caller to dial 5 to leave a message.
Skip greeting: Do not play a greeting.
Play busy greeting: play the extension busy greeting.
Play Unavailable greeting: play the extension Unavailable greeting.

c) Playback Options

**·Announce Message Caller ID**

If this option is enabled, the Caller ID of the party that left the message will be played back before the voicemail message begins playing.

**·Announce Message Duration**

If this option is set, the duration of the message in minutes will be played back before the voicemail message begins playing.

**.Announce Message Arrival Time**

If this option is set, the arrival time of the message will be played back before the voicemail message begins playing.

**.Allow Users to Review Messages**

Allow callers to review their recorded message before sending it to voicemail.

2) SMTP Settings for Voicemail

**Note**: If you want to send voicemail messages as email attachments, please configure this section.

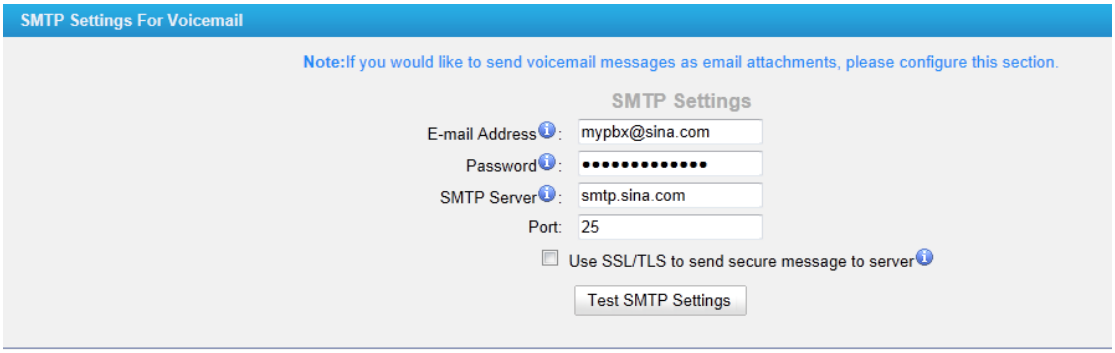



Figure 6-48

**·E-mail Address**

The E-mail Address that mPBX will use to send voicemail.

**·Password**

The password for the email address used above

**·SMTP Server**

The IP address or hostname of an SMTP server that the mPBX will connect to in order to send voicemail messages via email, i.e. mail.yourcompany.com.

**·Port**

SMTP Port: the default value is 25.

**·Use SSL/TLS to send secure message to server**

If the server of sending email needs to authenticate the sender, you need to select the check box.

**Note**: Must be selected for Gmail or exchange server.

After filling out the above information, you can click on the 'Test Account Settings' button to check whether the setup is OK.

1) If the test is successful, you can use the email safely.

2) If test failed, please check the above information is correct or network is

proper.

# 6.7 Advanced Settings

## 6.7.1 SIP Settings

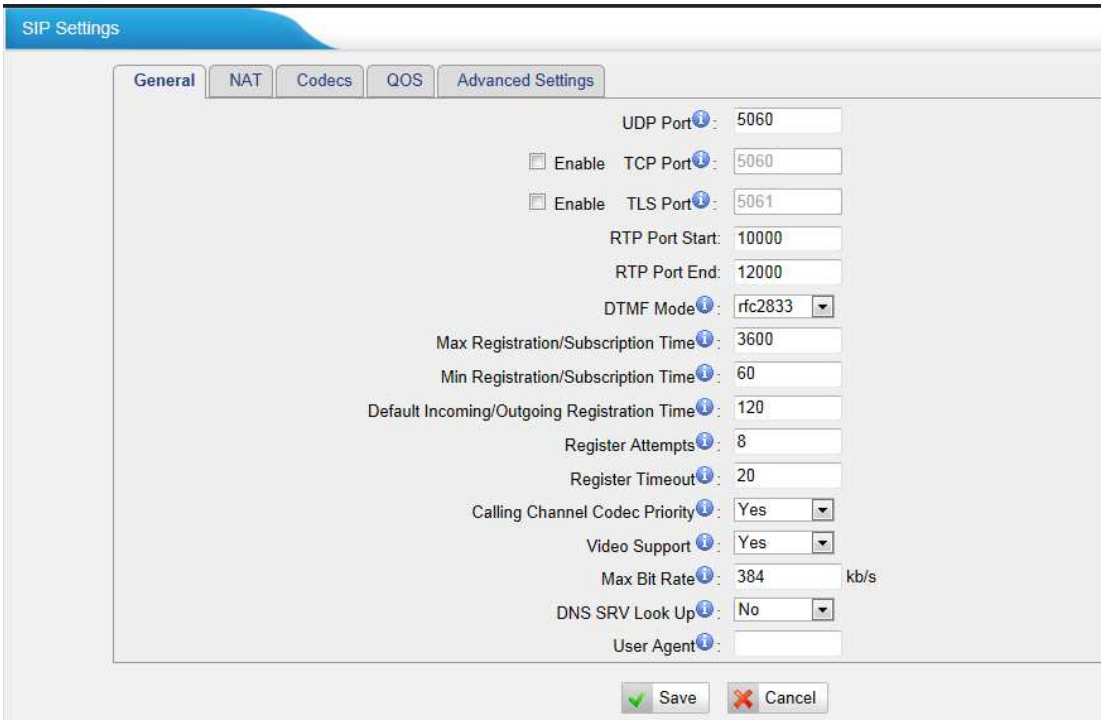



Figure 6-49

1) General

**·UDP Port**

Port use for sip registrations, Default is 5060.

**·TCP Port**

Port use for sip registrations, Default is 5060.

**·TLS Port**

Port use for sip registrations, Default is 5061.

**·RTP Port Start**

Beginning of RTP port range

**·RTP Port End**

End of RTP port range

**·DTMF Mode**

Set default mode for sending DTMF. Default setting: rfc2833

**·Max Registration/Subscription Time**
Maximum duration (in seconds) of a SIP registration. Default is 3600 seconds.

**·Min Registration/Subscription Time**
Minimum duration (in seconds) of a SIP registration. Default is 60seconds.

**·Default Incoming/Outgoing Registration Time**
Default Incoming/Outgoing Registration Time: Default duration (in seconds) of incoming/outgoing registration.

**·Register Attempts**
The number of SIP REGISTER messages to send to a SIP Registrar before giving up. Default is 8 times.

**·Register Timeout**
Number of seconds to wait for a response from a SIP Registrar before timed out . Default is 20 seconds.

**·Calling Channel Codec Priority**
Once enabled, when dialing out via SIP/SPS trunks, the codec of calling channel will be selected in preference. If not, mPBX will follow the priority in your SIP/SPS trunks.

**·Video Support**
Support for SIP video or no. Default is yes.

**·Max Bit Rate**
Configure the max bit rate for video stream. The default: 384kb/s

**·DNS SRV Look Up**
Please enable this option when your SIP trunk contains more than one IP address.

**·User Agent**
To change the user agent parameter of asterisk, the default is 'mPBX', you should change it if needed.

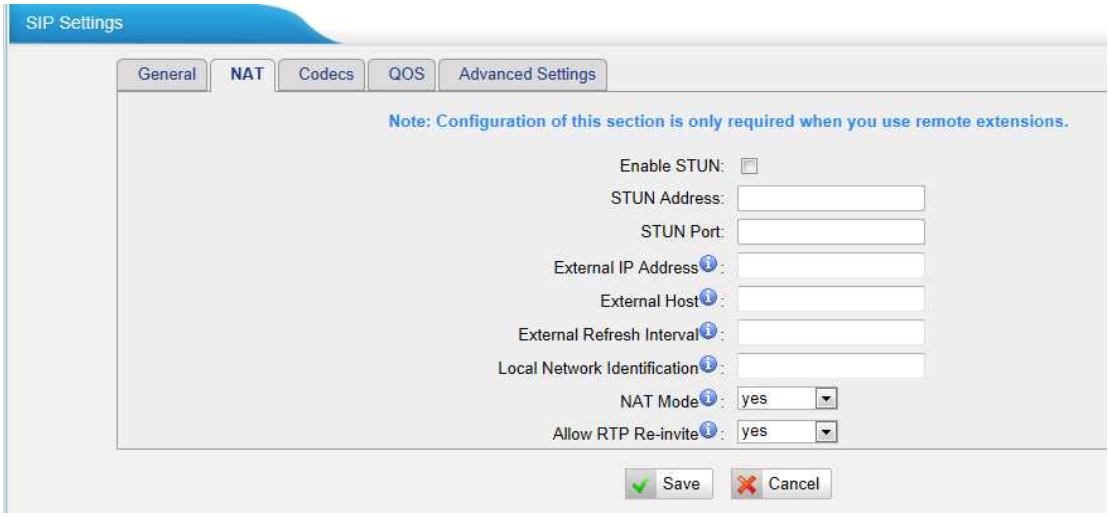



Figure 6-50

2) NAT

**Note**: Configuration of this section is only required when using remote extensions.

**·Enable STUN**

STUN (Simple Traversal of UDP through NATs) is a protocol for assisting devices behind a NAT firewall or router with their packet routing.

**·STUN Address**

The STUN server allows clients to find out their public address, the type of NAT they are behind and the internet side port associated by the NAT with a particular local port. This information is used to set up UDP communication between the client and the VOIP provider and so establish a call.

**·External IP Address**

The IP address that will be associated with outbound SIP messages if the system is in a NAT environment.

**·External Host**

Alternatively you can specify an external host, and the system will perform DNS queries periodically.

This setting is only required when your public IP address is not static. It is recommended that a static public IP address be used with this system. Please contact your ISP for more information.

**·External Refresh Interval**

If an external host has been supplied, you may specify how often the system will perform a DNS query on this host. This value is specified in seconds.

**·Local Network Identification**

Used to identify the local network using a network number/subnet mask pair when the system is behind a NAT or firewall.
Some examples of this are as follows:
'192.168.0.0/255.255.0.0' : All RFC 1918 addresses are local networks;
'10.0.0.0/255.0.0.0' : Also RFC1918;
'172.16.0.0/12':AnotherRFC1918withCIDRnotation;
'169.254.0.0/255.255.0.0' : Zero conf local network.
Please refer to RFC1918 for more information.

**·NAT Mode**
Global NAT configuration for the system. The options for this setting are as follows:
Yes = Use NAT. Ignore address information in the SIP/SDP headers and reply to the sender's IP address/port.
No = Use NAT mode only according to RFC3581.
Never = Never attempt NAT mode or RFC3581 support.
Route = Use NAT but do not include report in headers.

**·Allow RTP Reinvite**
By default, the system will route media steams from SIP endpoints through itself. Enabling this option causes the system to attempt to negotiate the endpoints to route packets to each other directly, bypassing the system. It is not always possible for the system to negotiate endpoint-to-endpoint media routing.

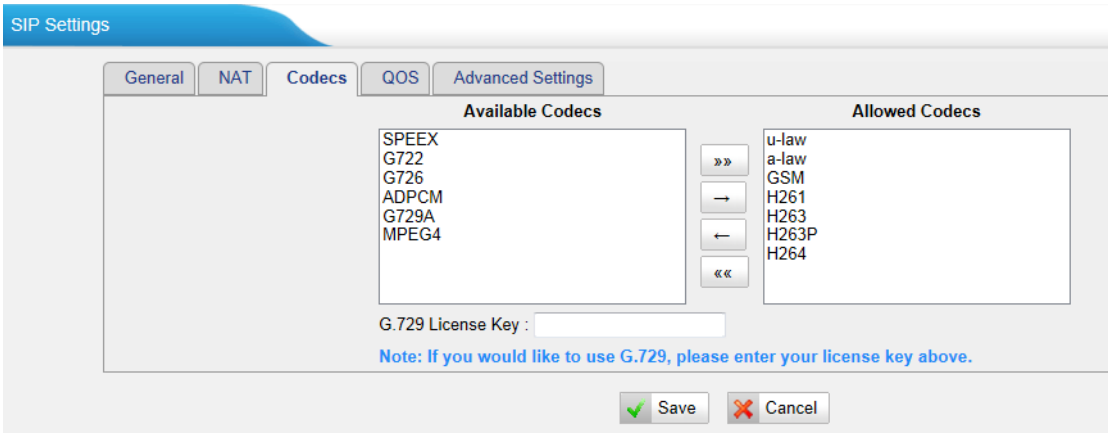



Figure 6-51

3）Codecs
A codec is a compression or decompression algorithm that used in the transmission of voice packets over a network or the Internet.
**u-law:** A PSTN standard codec, used in North America, that provides very good voice quality and consumes 64kbit/s in each direction (receiving and transmitting) of a VoIP call.

**a-law:** A PSTN standard codec, used outside of North America, that provides very good voice quality and consumes 64kbit/s in each direction (receiving and transmitting) of a VoIP call.

**GSM:** A wireless standard codec, used worldwide, that provides adequate voice quality and consumes 13.3kbit/s in each direction (receiving and transmitting) of a VoIP call. GSM is supported by many VoIP phones.

**SPEEX:** Speex is an Open Source/Free Software patent-free audio compression format designed for speech. The Speex Project aims to lower the barrier of entry for voice applications by providing a free alternative to expensive proprietary speech codecs. Moreover, Speex is well-adapted to Internet applications and provides useful features that are not present in most other codecs.

**G.722:**G.722 is a wideband speech coding algorithms which supports the bit rate of 64, 56 and 48kbps wideband. It's a broadband voice encoding of G series.

**G.726:** A PSTN codec, used worldwide, that provides good voice quality and consumes 32kbit/s in each direction (receiving and transmitting) of a VoIP call. G.726 is supported by some VoIP phones.

**ADPCM, G.729A, H261, H263, H263p, H264,MPEG4**.
**Note:** If you would like to use G.729, please enter your license.

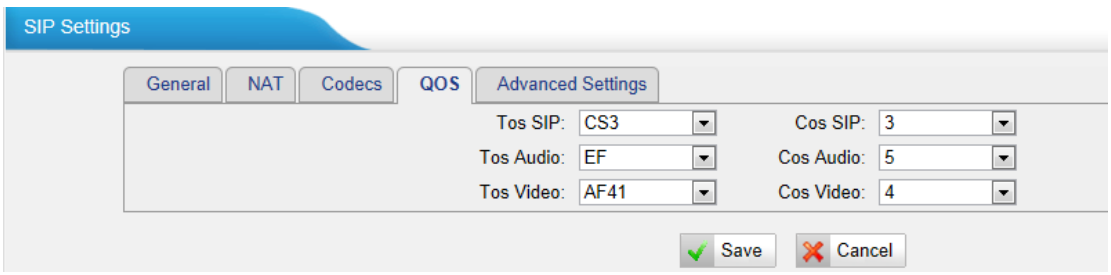



Figure 6-52

4）QOS

QoS (Quality of Service) is a major issue in VOIP implementations. The issue is how to guarantee that packet traffic for a voice or other media connection will not be delayed or dropped due interference from other lower priority traffic. When the network capacity is insufficient, QoS could provide priority to users by setting the value.

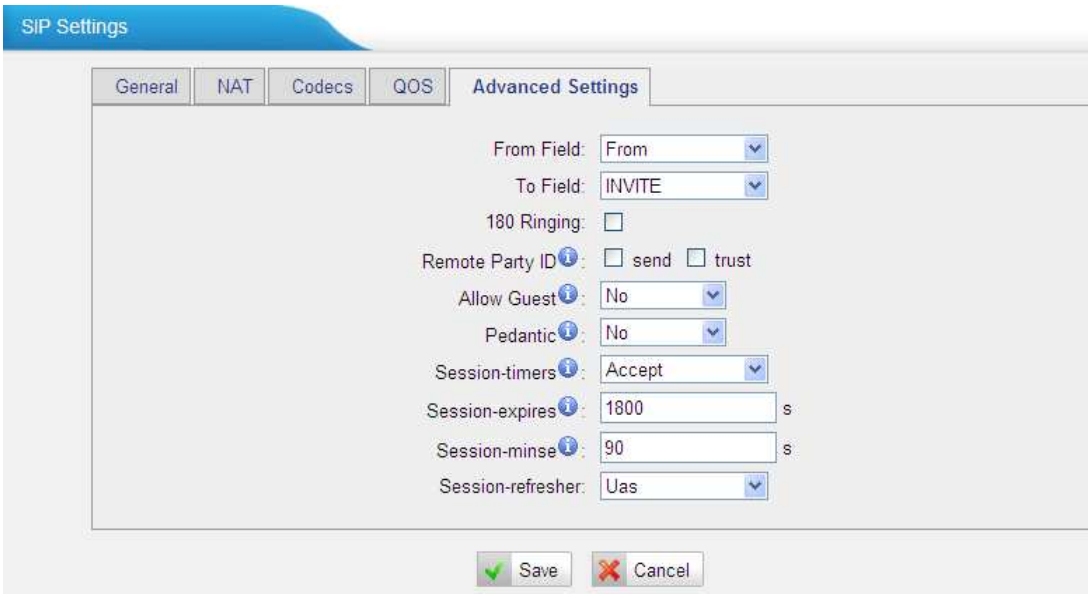



Figure 6-53

5) Advanced Settings

**·From Field**

Where to get the caller ID in sip packet.

**·To Field**

Where to get the DID in sip packet.

**·180 Ringing**

It is set when the telecom provider needs. Usually it is not needed.

**·Qualify**

Send check alive packets to the sip provider.

**·Remote Party ID**

Whether send Remote-Party-ID on SIP header. Default no.

**·Allow Guest**

Whether allow anonymous registration extension. Default: no.

This option is used to avoid some anonymous calls by hackers. More details for the system security configuration, please refer to **APPENDIX G mPBX Security Configuration Guide.**

**·Pedantic**

Enable pedantic parameter. Default: no.

**·Session -timers**

Enable sesstion-timer mode, default: yes

**·Sesstion-expires**
The max refresh interval

**·Sesstion-minse**
The min refresh interval, which mustn't be less than 90s

**·Sesstion-refresher**
Choose sesstion-refersher, the default is Uas

## 6.7.2 IAX Settings

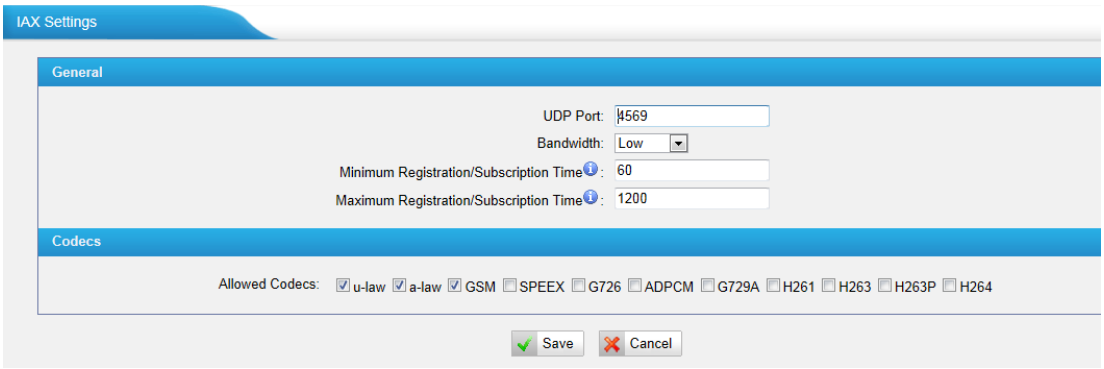



Figure 6-54

**1) General**

**·Bind Port**
Port use for IAX2 registrations, Default is 4569.

**·Bandwidth**
Low/medium/high with this option you can control which codec to be used.

**·Min Registration Time**
Minimum duration (in seconds) of a IAX2 registration. Default is 60seconds.

**·Max Registration Time**
Maximum duration (in seconds) of a IAX2 registration. Default is 1200 seconds.

2）Codecs
A codec is a compression or decompression algorithm that used in the transmission of voice packets over a network or the Internet.
**u-law:** A PSTN standard codec, used in North America, that provides very good voice quality and consumes 64kbit/s in each direction (receiving and transmitting) of a VoIP call.

**a-law:** A PSTN standard codec, used outside of North America, that provides very good voice quality and consumes 64kbit/s in each direction (receiving and transmitting) of a VoIP call.

**GSM:** A wireless standard codec, used worldwide, that provides adequate voice quality and consumes 13.3kbit/s in each direction (receiving and transmitting) of a VoIP call. GSM is supported by many VoIP phones.

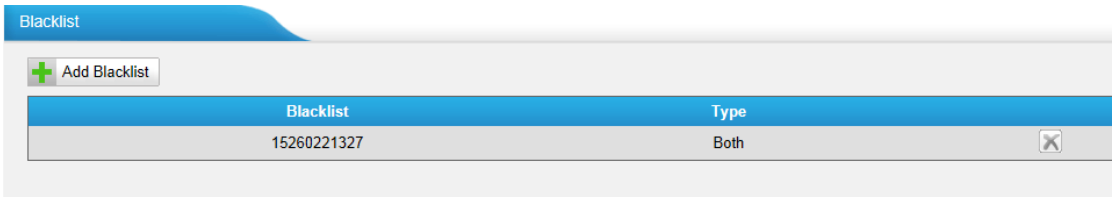
**SPEEX:** Speex is an Open Source/Free Software patent-free audio compression format designed for speech. The Speex Project aims to lower the barrier of entry for voice applications by providing a free alternative to expensive proprietary speech codecs. Moreover, Speex is well-adapted to Internet applications and provides useful features that are not present in most other codecs.

**G.726:** A PSTN codec, used worldwide, that provides good voice quality and consumes 32kbit/s in each direction (receiving and transmitting) of a VoIP call. G.726 is supported by some VoIP phones.

**ADPCM, G.729A, H261, H263, H263p, H264**.
**Note:** If you would like to use G.729, please enter your license.

## 6.7.3 Blacklist

Blacklist is used to block an incoming/outgoing call. If the number of incoming/outgoing call is registered in the number blacklist, the caller will hear the following prompt: "The number you have dialed is not in service. Please check the number and try again". The system will then disconnect the call.




We can add a number with the type: inbound, outbound or both

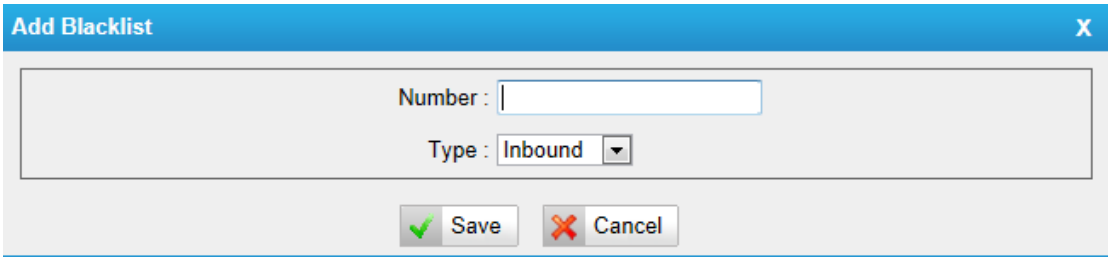



Figure 6-55

**Note:** It will not working for internal extension number.

## 6.7.4 Callback Settings

mPBX allows caller A to dial an inbound route number, and after hearing the ring, A can hang up the call or wait for mPBX to cut off the call, then mPBX will call A with this number. When a pick up the call, A can dial the number he wants to call; mPBX will call the number with its outbound route.

**Note:**

1. If you'd like to use callback feature, please make sure if it's enabled on the inbound route setting panel.
2. No callback rules needed to be set if the trunk supports call back with the caller ID directly.

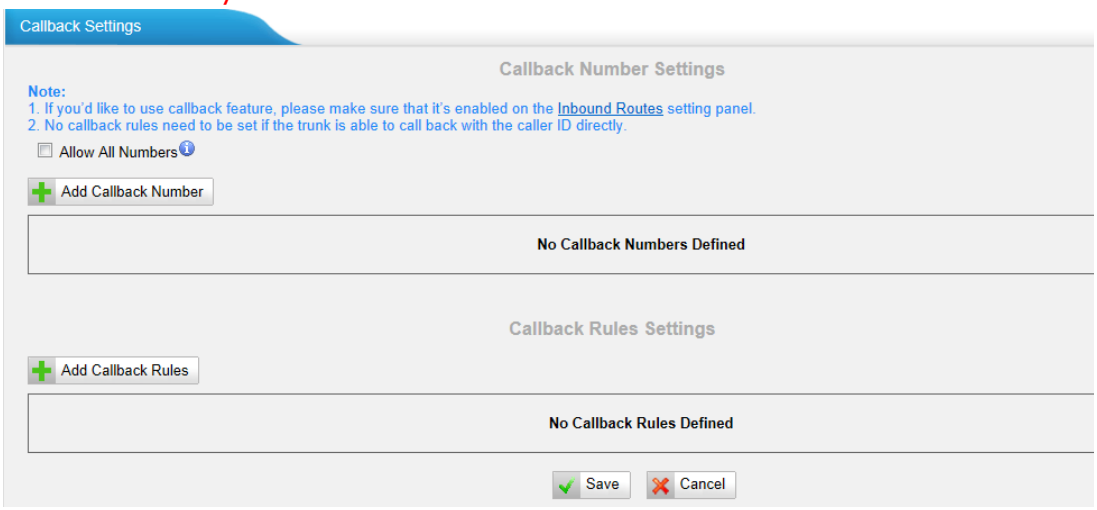

Callback Settings
Callback Number Settings
Note:
1. If you'd like to use callback feature, please make sure that it's enabled on the Inbound Routes setting panel.
2. No callback rules need to be set if the trunk is able to call back with the caller ID directly.
Allow All Numbers
Add Callback Number
No Callback Numbers Defined
Callback Rules Settings
Add Callback Rules
No Callback Rules Defined
Save
Cancel

Figure 6-56

**·Allow All Numbers**

If you want to apply Callback function to all incoming numbers, please tick Allow All numbers.

Follow the step to use this function.

Step 1: Enable Callback.

Inbound Routes –Choose "Yes" on "Enable Callback" to enable this function

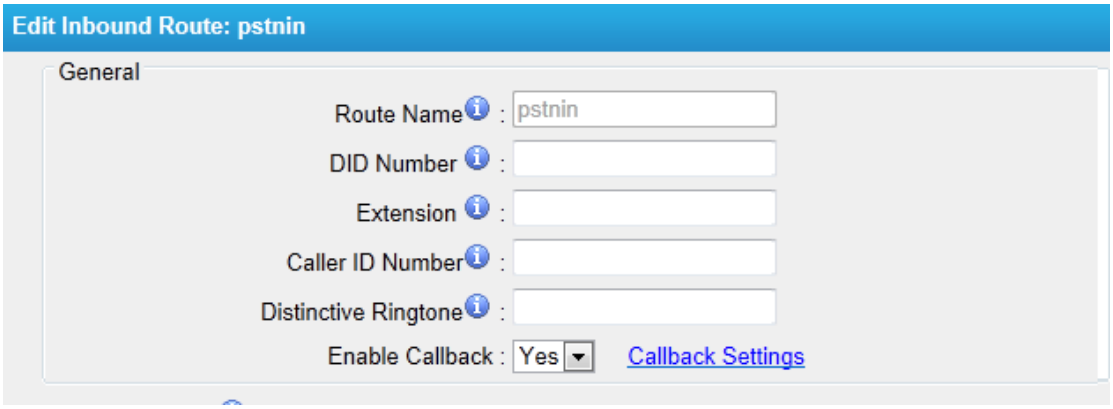



Figure 6-57

Step 2: Create Callback number

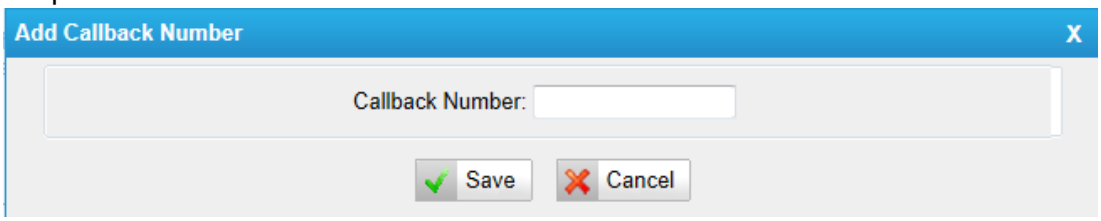



Figure 6-58

Step 3: Create Callback Rules

You will need to create callback rules when the system should strip or add digits.

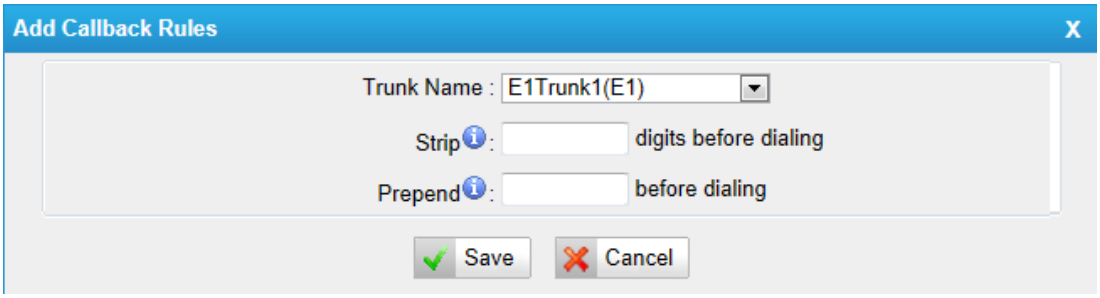



Figure 6-59

**·Trunk Name**

Choose the trunk with callback rules

**·Strip digits from front**

Define how many digits will be stripped from the call in number before the callback is placed. For example, when you call from number 123456789 into mPBX, the caller ID is 0123456789, but you can only call 123456789 successfully from mPBX trunk. You should configure number 0123456789 as the call back number and strip 1 digit before the callback is placed

**·Prepend before dialing**

Define digits added before a callback number before the callback is placed. For example, the call in number (Caller ID) is 123456789, mPBX need to send 9123456789 to its trunk when call to this number. You should configure 123456789 as the call back number and add 9 before the callback is placed. You can add 'w' for analog trunks for some delay too

## 6.7.5 DNIS Settings

DNIS (Dialed Number Identification Service) is a telephone service that identifies for the receiver of a call the number that the caller dialed

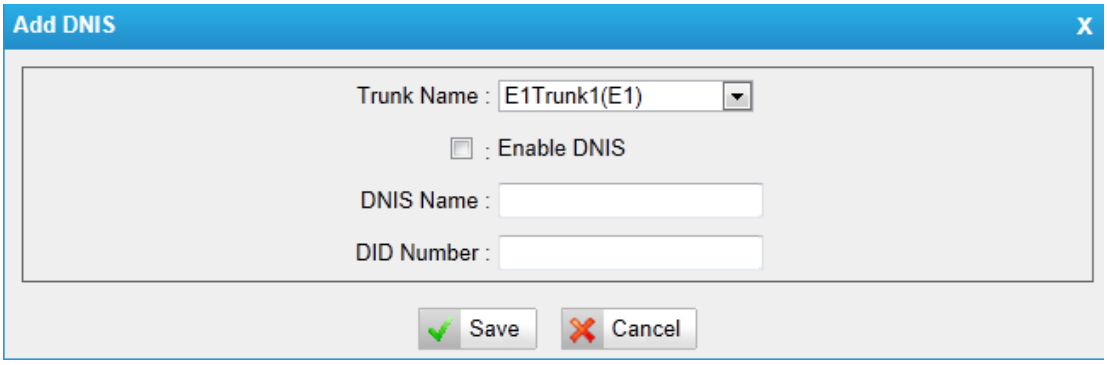



Figure 6-60

**Note:** If DID is not configured here, all the calls via this trunk will show the DNIS instead of the original caller ID

## 6.7.6 DISA

DISA (Direct Inward System Access) allows someone calling in from outside the telephone switch (PBX) to obtain an 'internal' system dial tone and make calls as if they were using one of the extensions attached to the telephone switch. To use DISA, a user calls a DISA number, which invokes the DISA application. The DISA application in turn requires the user to enter a PIN number, followed by the pound sign (#). If the PIN number is correct, the user will hear dial tone on which a call may be placed. Obviously, this type of access has serious security implications, and great care must be taken not to compromise your security

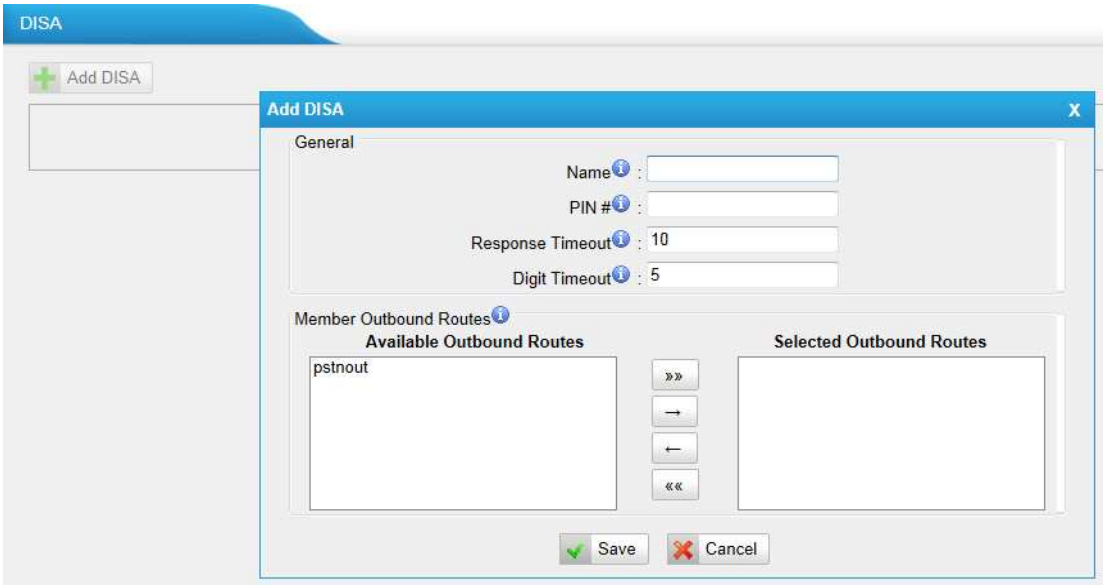



Figure 6-61

1) General

**·DISA Name**
Give this DISA application a name to help you identify it.
**·PIN#**
The password for this DISA .
**·Response Timeout**
The maximum amount of time the system will wait before hanging up the call if the user has dialed an incomplete or invalid number. Default is 10 seconds.
**·Digit Timeout**
The maximum amount of time permitted between each digit when the user is dialing an extension number. Default is 5 seconds.

2) Member Outbound Routes
Used to set the outbound routes that can be accessed from this DISA.

## 6.7.5 PIN User Settings

PIN User is used to manage lists of PINs that can be used to access restricted features such as Outbound Routes.

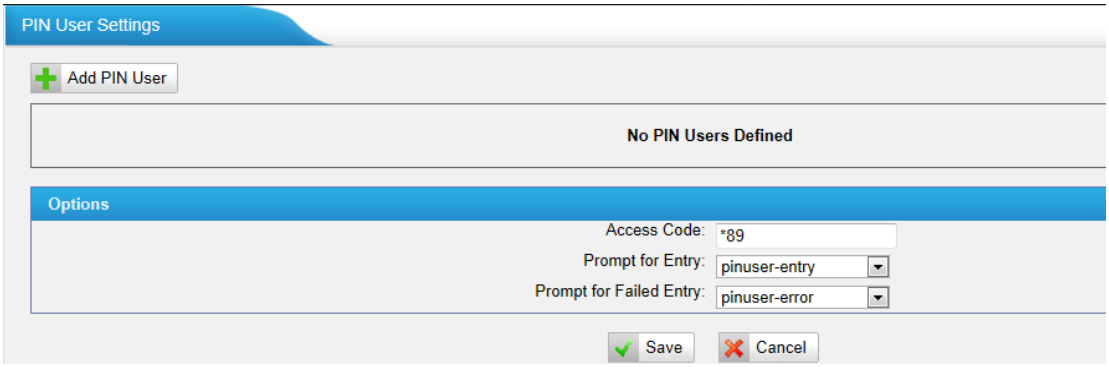



Figure 6-62

1) Options
**·Access Code**
.Dial this code to access PIN.

**·Prompt for Entry**
Prompt caller enter the PIN Number.

**·Prompt for Entry Failure**
Prompt the caller when an invalid PIN is entered.

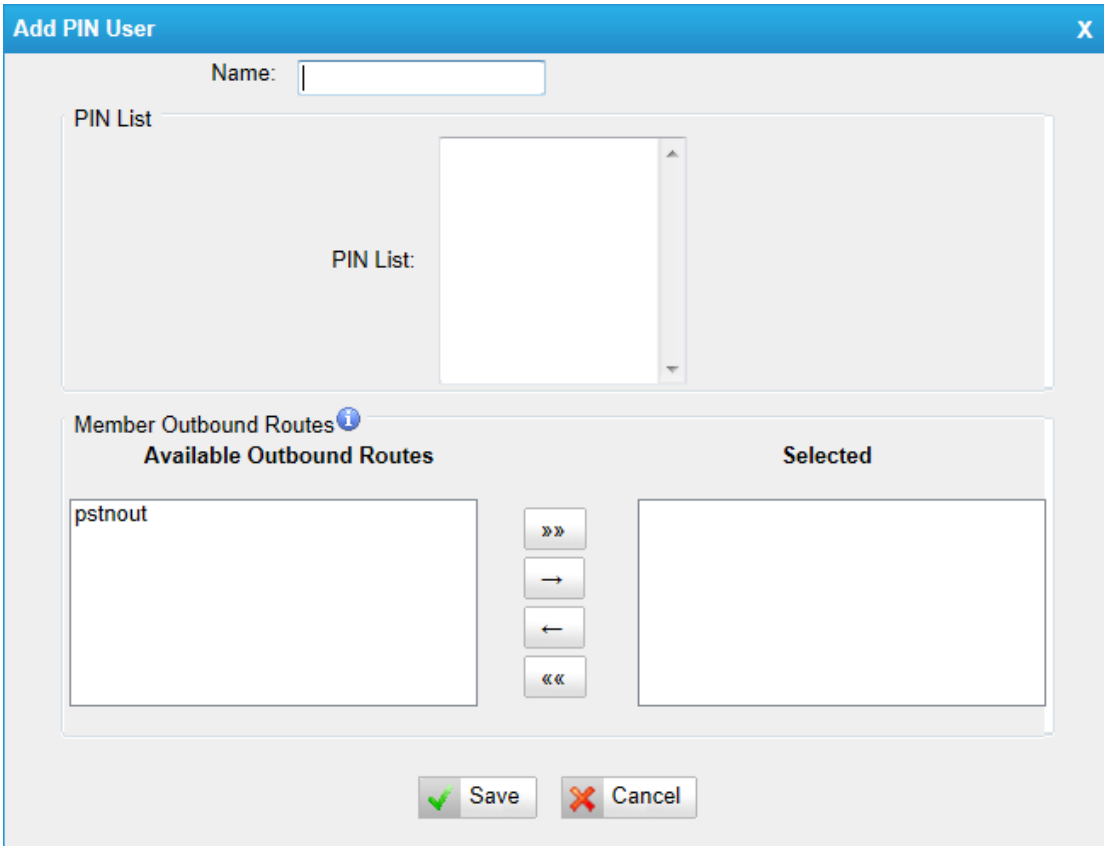



Figure 6-63

2) PIN User

mPBX can store a number of PIN Users. PIN Users may be used to keep track of calls in relation to particular activities or clients. They can also be used to keep track of calls by particular users or sets of users.

• PIN entered are checked against those stored by the system. If an invalid PIN is entered, the PIN is requested again.
• The system administrator can configure certain numbers or types of numbers to require entry of a PIN before you can continue making a call to such a number.
• The system administrator can also configure you to have to enter a PIN before making any external call.

**·Name**

A character-based name for this PIN list, i.e. 'Yeastar PIN'

**·PIN List**

Enter a list of one or more PINs, One PIN per line.

**·Outbound Route**

PIN User can use those outbound route to make call out

## 6.7.8 Paging Groups

Paging is used to make an announcement over the speakerphone to a phone or group of phones. Targeted phones will not ring, but instead answer immediately into speakerphone mode. Please note that this section is for configuring paging groups. If you would like to configure Intercom settings, please open the Other Settings -> Feature Codes screen.
This feature is supported by the following SIP phones:
Yealink's T28, T26,T22,T20,T10T,T9CM. Other SIP devices may also work with this feature but are not officially supported.
**Note**: A paging group can have a maximum of 20 members.

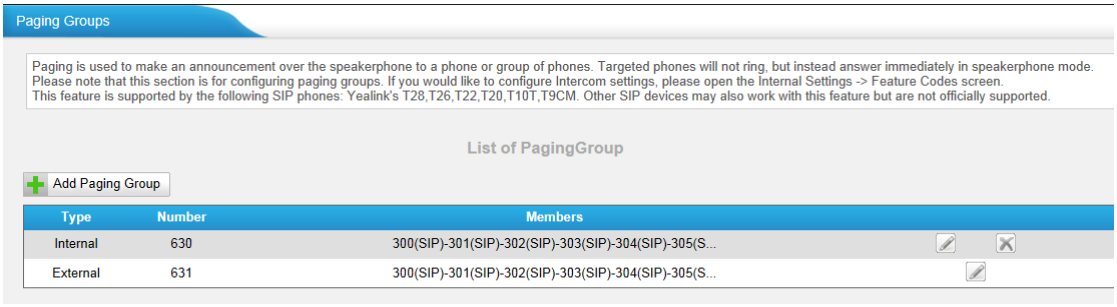

Paging Groups
Paging is used to make an announcement over the speakerphone to a phone or group of phones. Targeted phones will not ring, but instead answer immediately in speakerphone mode.
Please note that this section is for configuring paging groups. If you would like to configure Intercom settings, please open the Internal Settings -> Feature Codes screen.
This feature is supported by the following SIP phones: Yealink's T28,T26,T22,T20,T10T,T9CM. Other SIP devices may also work with this feature but are not officially supported.
List of PagingGroup
Add Paging Group
Type
Number
Members
Internal
630
300(SIP)-301(SIP)-302(SIP)-303(SIP)-304(SIP)-305(S...
External
631
300(SIP)-301(SIP)-302(SIP)-303(SIP)-304(SIP)-305(S...

Figure 6-64

There are two types of paging groups in WELL mPBX-U110R
1. Internal paging Group
In this mode, if you dial its number, mPBX will help to pick up those chosen members and you can talk directly without any rings.

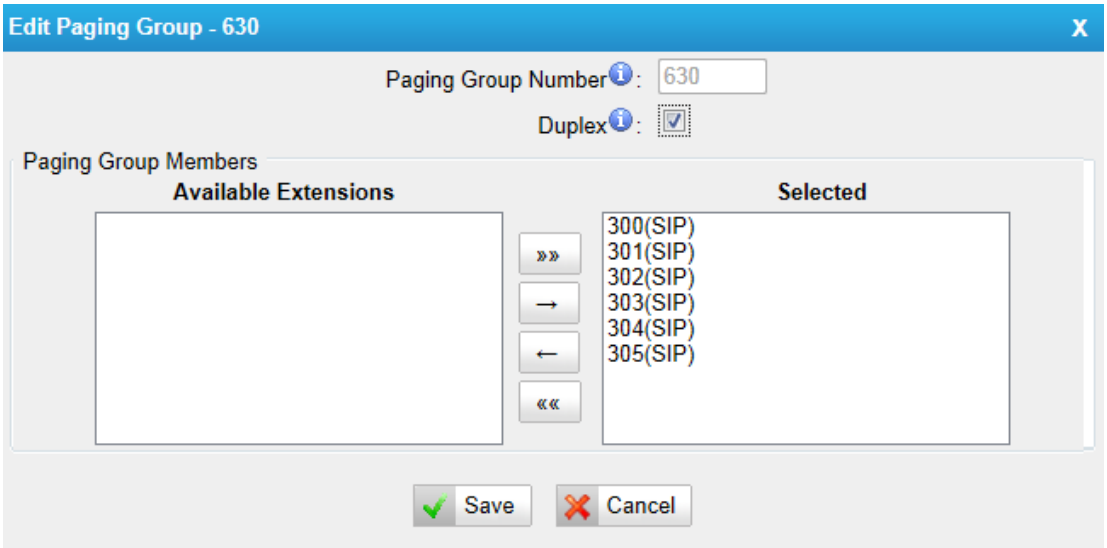



Figure 6-65

**·Paging Group Number**
Define the numbered extension that may be dialed to reach this group.

**·Duplex**

Paging is typically one way for announcements only. Checking this will make paging duplex, allowing all users in the group to talk and be heard by all.

2. External paging group

In this mode, the chosen extensions will have the rights to dial the group number, all his voice will be broadcasted via the 'Audio Out' interface of U300

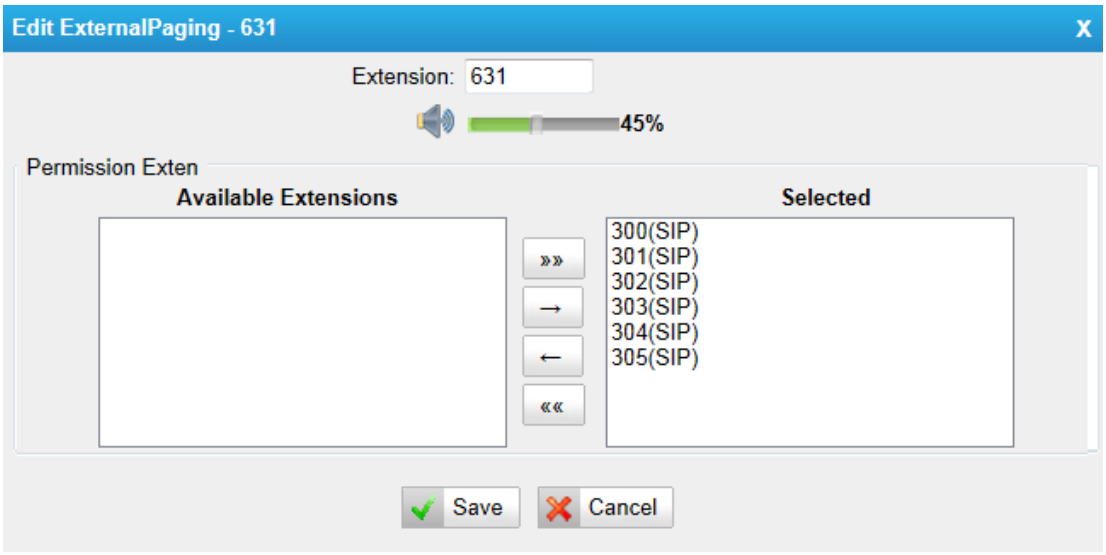



Figure 6-66

# 7 Reports

Click

to access
We can check the call detailed logs for counting and system log for debugging

## 7.1 Call Logs

The call Log captures all call details, including call time, caller number, callee number, call type, call duration, etc. An administrator can search and filter call data by filter the call logs by call date, caller/callee, trunk, duration, billing duration, status, communication type, Pin User.

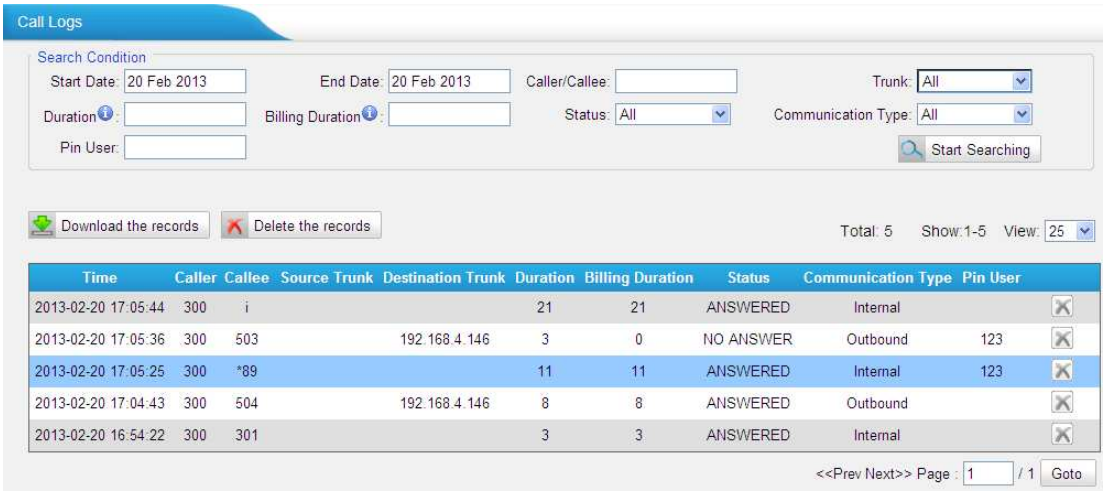

Call Logs
Search Condition
Start Date: 20 Feb 2013
End Date: 20 Feb 2013
Caller/Callee:
Trunk: All
Duration:
Billing Duration:
Status: All
Communication Type: All
Pin User:
Start Searching
Download the records
Delete the records
Total: 5
Show:1-5
View: 25
Time Caller Callee Source Trunk Destination Trunk Duration Billing Duration Status Communication Type Pin User
2013-02-20 17:05:44 300 i 21 21 ANSWERED Internal
2013-02-20 17:05:36 300 503 192.168.4.146 3 0 NO ANSWER Outbound 123
2013-02-20 17:05:25 300 *89 11 11 ANSWERED Internal 123
2013-02-20 17:04:43 300 504 192.168.4.146 8 8 ANSWERED Outbound
2013-02-20 16:54:22 300 301 3 3 ANSWERED Internal
<<Prev Next>> Page : 1 / 1 Goto

Figure 7-1

## 7.2 System Logs

You can download and delete the system logs of mPBX

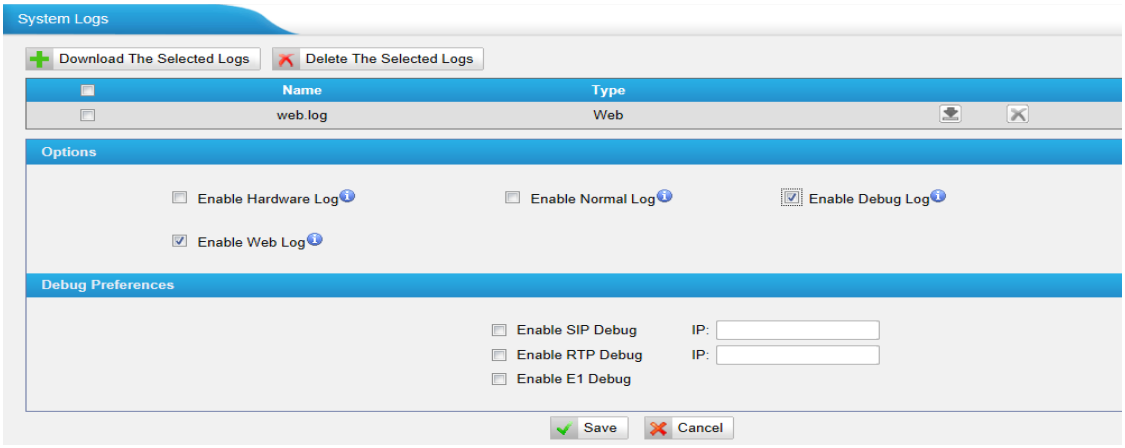


Figure 7-2

Options

**·Enable Hardware Log**

Save the information of hardware; (up to 4 log files)

**·Enable Normal Log**

Save the prompt information; (up to 16 log files)

**·Enable Web Log**

Save the history of web operations (up to 2 log files)

**·Enable Debug Log**

Save debug information (up to 2 log files)

We can also enable the SIP/RTP/E1 debug, it's very useful for checking problems.

2） Packet Capture Tool

This feature always used to capture packets for technician. Integrate packet capture tool 'Wireshark' in mPBX.

Users also could specify the destination IP address and port to get the packets.

**·IP**

Specify the destination IP address to get the packets.

**·Port**

Specify the destination Port to get the packets.

# 8 Logout

Click

to log out safely to the log in page.

# 9. Use mPBX

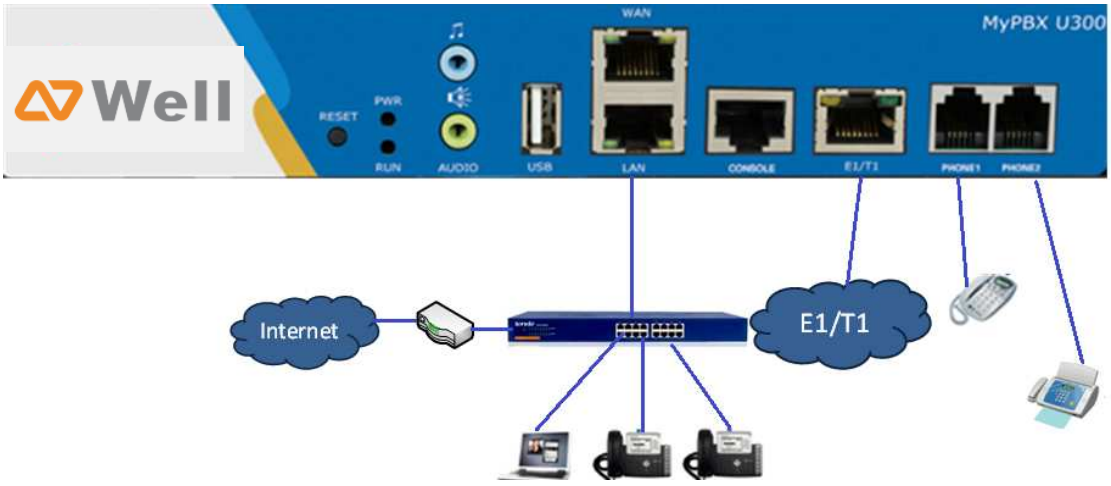



Figure 9-1

## 9.1 Make outbound call

To make an outbound call, we need to add trunk first. There are 3 types of VoIP Trunk:

·**Digital Trunk:** E1/T/J1 ports of mPBX, connected to the ISDN provider.
You need to get the detailed signaling type from the provider before configure the E1 trunk.

·**VoIP Trunk:** Connected to remote VOIP service server.
You should get an IP address with user name/ password from the provider.

·**Service Provider:** Connected to service provider server.
You will get only IP address for authorization.

### 9.1.1 Sample Routing via E1 Trunk

Let's route all inside extensions through an E1 trunk by dialing 9. In Outbound Routes, add a new outbound route as below.

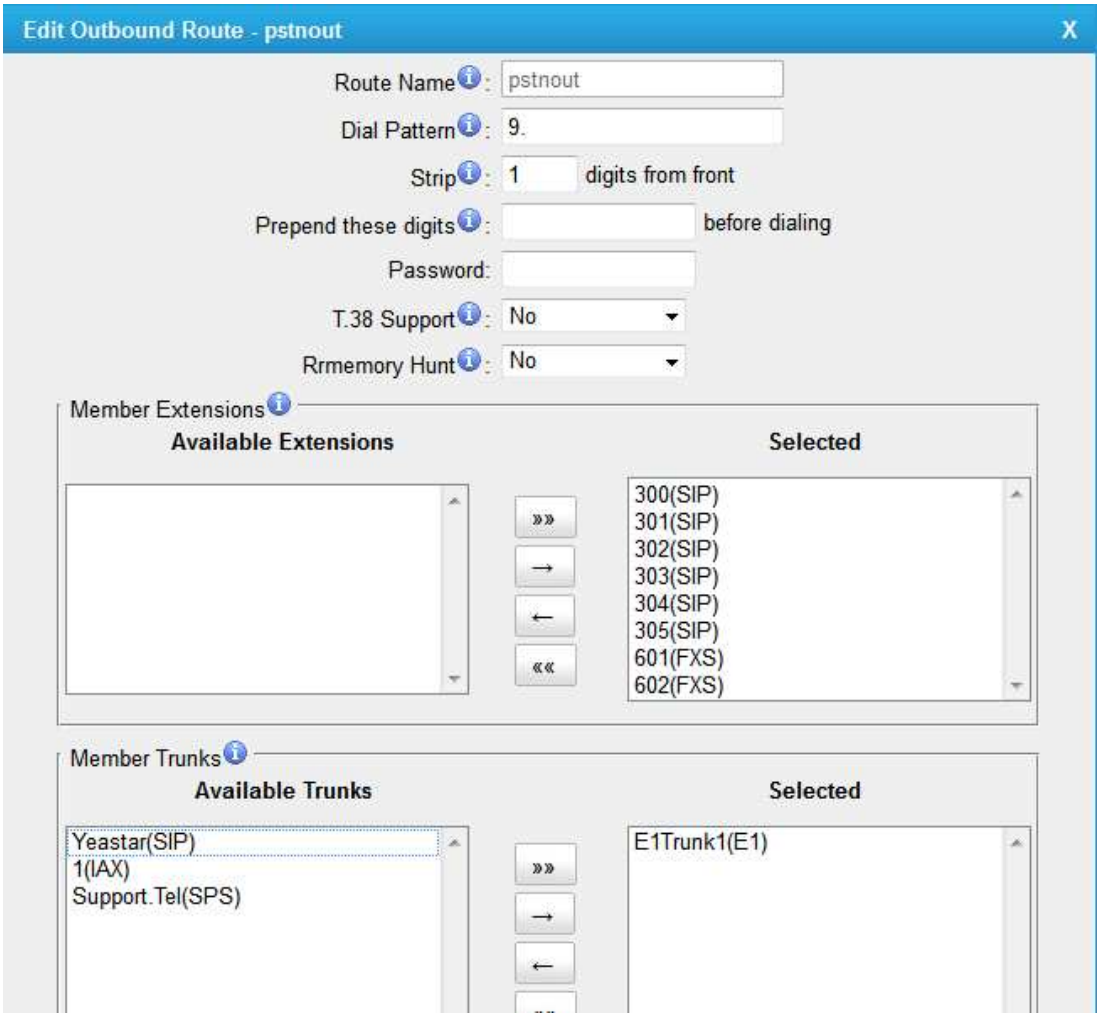



Figure 9-1

As we can see from the outbound route of 'pstnout', all phone numbers starting with 9 will have their first digit stripped off (digit 9) and will be sent to the E1.

After we have configured the above, we can dial 9 + local number to dial out via a E1 trunk.

**Note:** Setting number prefix to wild card X. and setting Strip to 0 digits from the front will allow all calls to go through this outbound route directly.

## 9.1.2 Sample Routing via VoIP Trunk

Let's configure all inside extensions to dial '0' through the VoIP Trunk.

**1. Add VoIP service provider**

Before we do add this, please make sure you have a VoIP Trunk account.

Trunks→VoIP Trunk →SIP Trunk

Enter your account information on this page, and click Save.

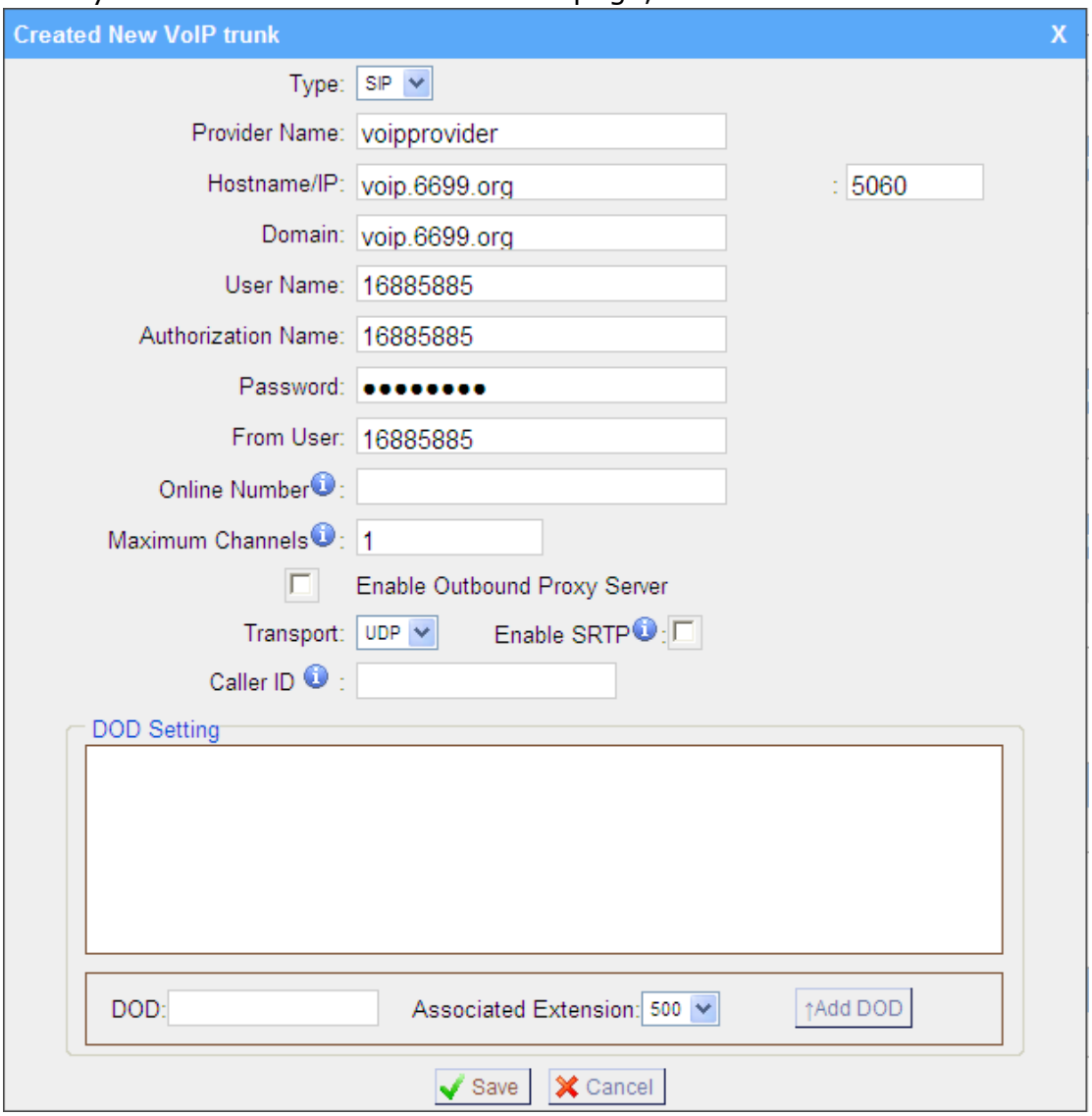



Figure9-2

**2. Add Outbound Routes**

As we can see from the Outbound Route of 'voipout', all phone numbers starting with 0will have their first digit stripped off (digit 0) and will be sent to the SIP Trunk.

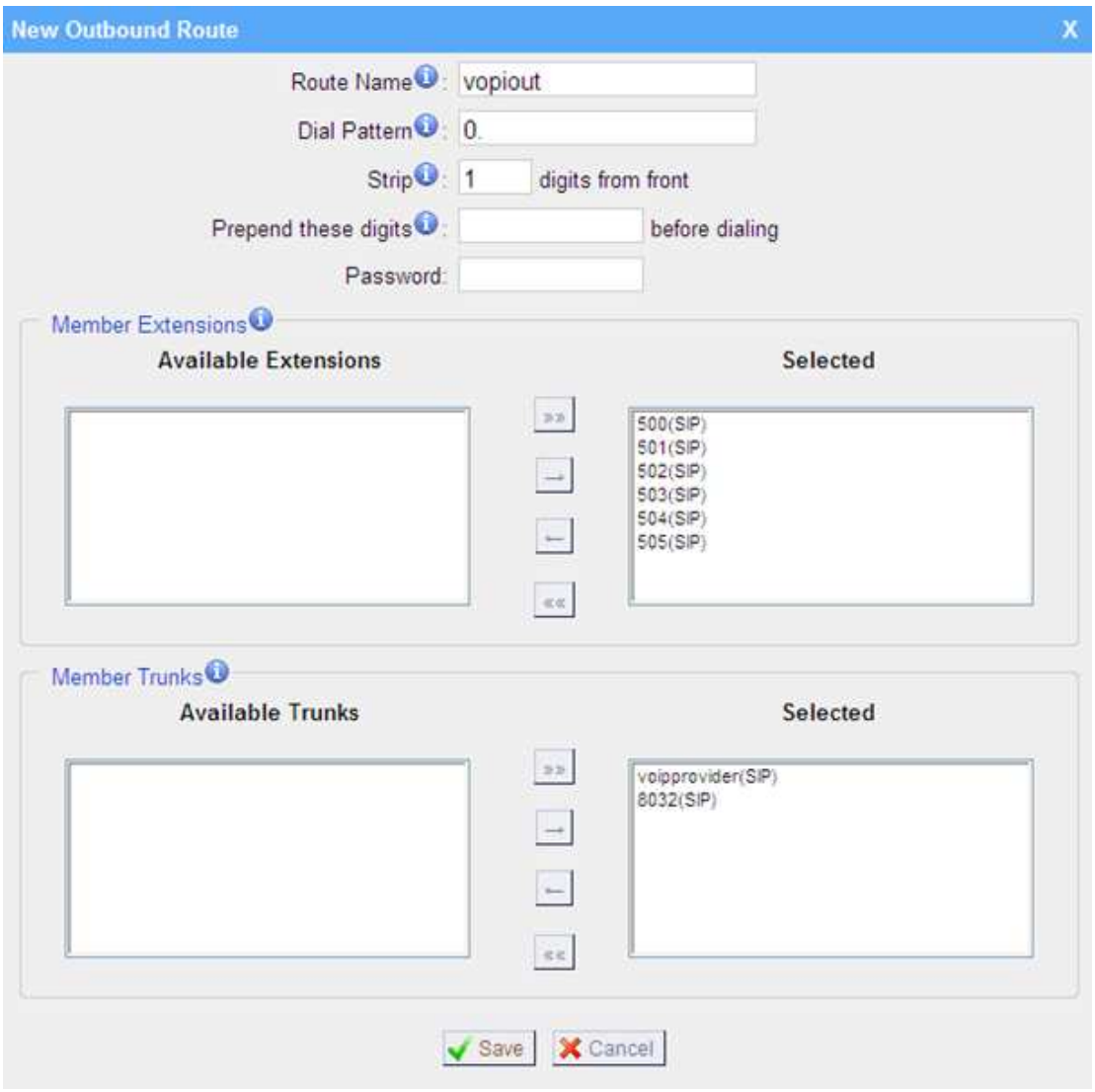



Figure9-3

Now that we have added two outbound dialing rules, any call starting with 9 will be routed to the PSTN, and any number starting with 0 will be routed to the SIP Trunk.

# 9.2 Incoming call

## 9.2.1 Sample Routing to an IVR

Let's configure an incoming call to route to the IVR. In the IVR itself, let's configure digit 0to route the call to extension 500, and digit 1 to route the call to extension 501.

**1. Add IVR**

To add a new IVR, go to IVR→ Create New IVR

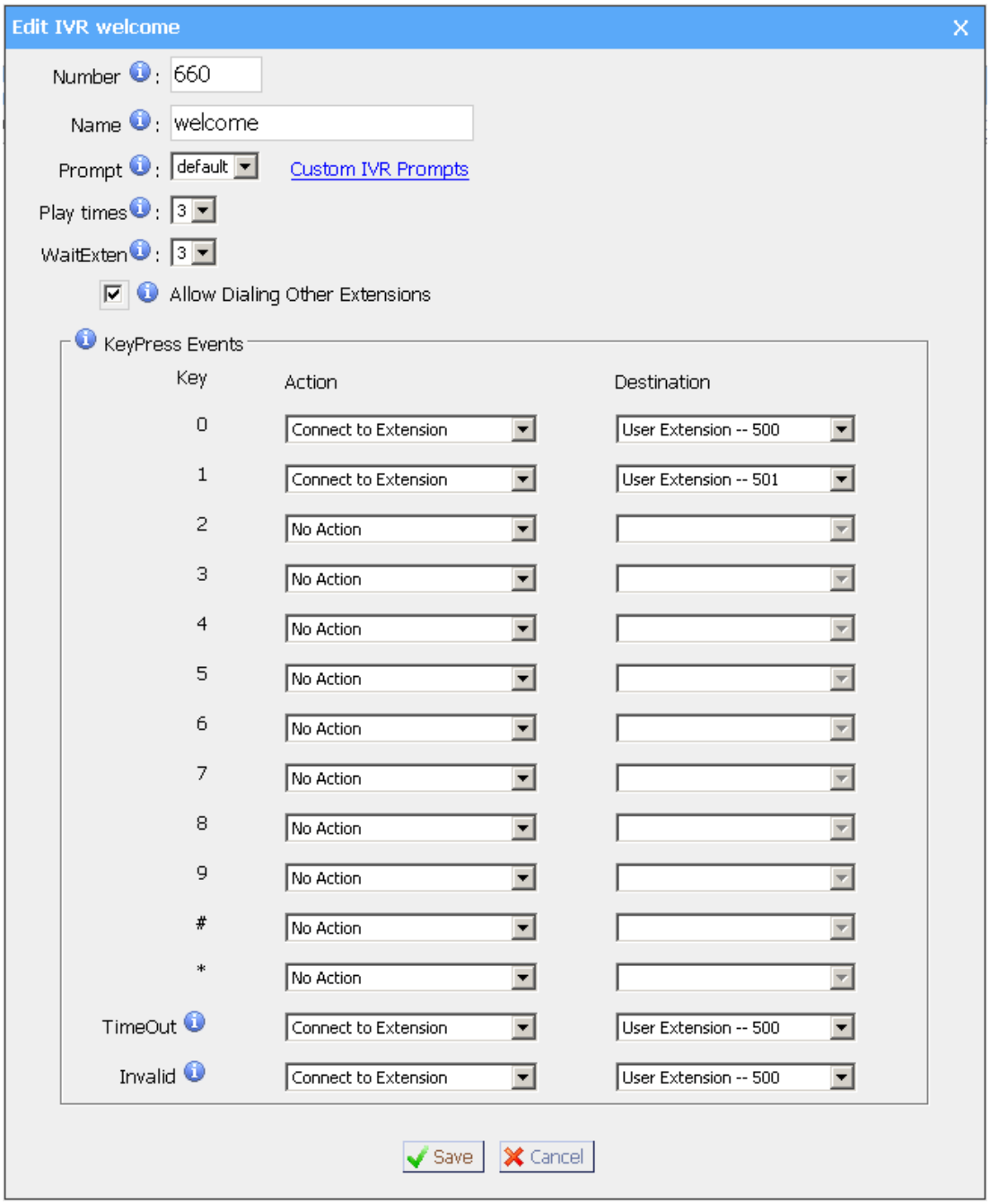



Figure9-4

**2. Add Inbound Routes**

As we can see from the Inbound Route of 'allin', all incoming calls will be sent to the IVR.

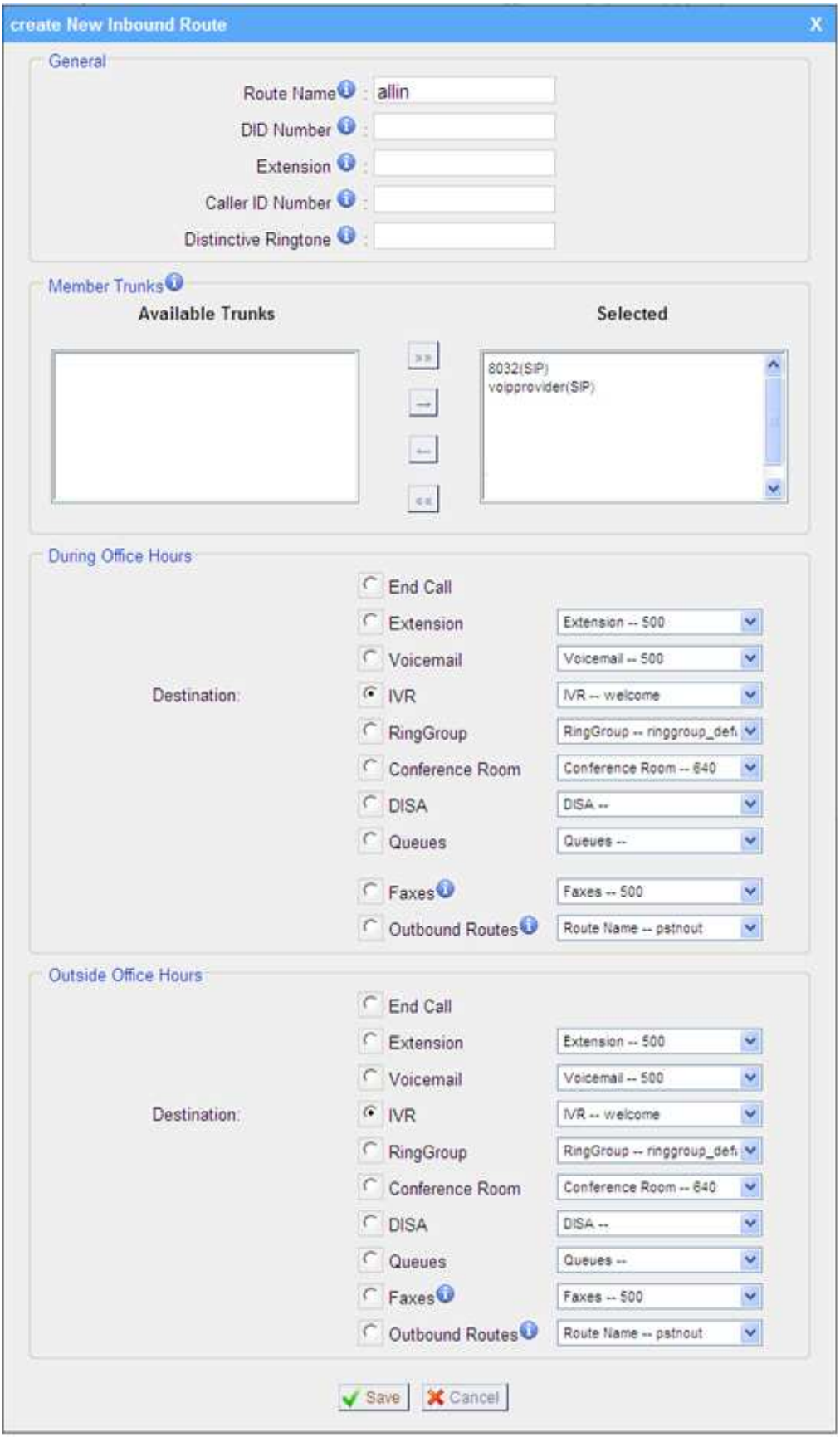

create New Inbound Route
X
General
Route Name : allin
DID Number :
Extension :
Caller ID Number :
Distinctive Ringtone :
Member Trunks
Available Trunks
Selected
8032(SIP)
voipprovider(SIP)
During Office Hours
Destination:
End Call
Extension
Extension -- 500
Voicemail
Voicemail -- 500
IVR
IVR -- welcome
RingGroup
RingGroup -- ringgroup_defi
Conference Room
Conference Room -- 640
DISA
DISA --
Queues
Queues --
Faxes
Faxes -- 500
Outbound Routes
Route Name -- pstnout
Outside Office Hours
Destination:
End Call
Extension
Extension -- 500
Voicemail
Voicemail -- 500
IVR
IVR -- welcome
RingGroup
RingGroup -- ringgroup_defi
Conference Room
Conference Room -- 640
DISA
DISA --
Queues
Queues --
Faxes
Faxes -- 500
Outbound Routes
Route Name -- pstnout
Save
Cancel

Figure9-5

# APPENDIX A FAQ

## Q1. How to Register SIP device?

**A1:**
1)Register SIP softphone
Download the x-lite softphone from counterpath website
www.counterpath.com
After install the x-lite, right click the panel and select the SIP Account setting and then configure it.
**Display Name**: 500
**User Name**: 500
**Password**: 500
**Authorization Name**: 500
**Domain**: 192.168.5.150

2) Register IP Phone (for example, Yealink's T28 IP Phone)
a) Connect the T28's Internet port to the switch. And it can get the IP from your route.
b) Press the 'OK' key on T28 to get the IP of T28.
c) Put the IP on web browser then you can enter the T28 configure page through this IP.
d) Put the SIP extensions info on the T28 IP phones.
**Display Name**: 501
**User Name**: 501
**Register Name**: 501
**Password**: 501
**SIP Server**: 192.168.5.150
Use the same method register another T28 to other extension.

## Q2. How do I reset mPBX back to the factory default settings?

**A2:** To perform a reset, please follow steps below:
**Step 1:**Hold downthe 'Reset' button on the back of the unit for 5 seconds and watch the LEDs on the front of the mPBX. When the status LED turns red, let go of the reset button.
**Step2:**When the RUN status LED starts blinking,mPBX will be set back to factory defaults.
**Step 3:** To access the configuration page, navigate to192.168.5.150using a web browser. Make sure that you are on the 192.168.5.0 subnet before doing this.
**Step4:** Login to the device with the username 'admin' and the password 'password', in order to begin reconfiguring the device.

# APPENDIX B How to Configure Autobackup

Before Autobackup can be properly configured, an SMB share folder accessible from mPBX must be set up on a Windows based machine. Once that has been set up, please follow the steps below.

**Step 1** Add a new folder, rename it, and set this new folder's share Properties according to Figure B-1

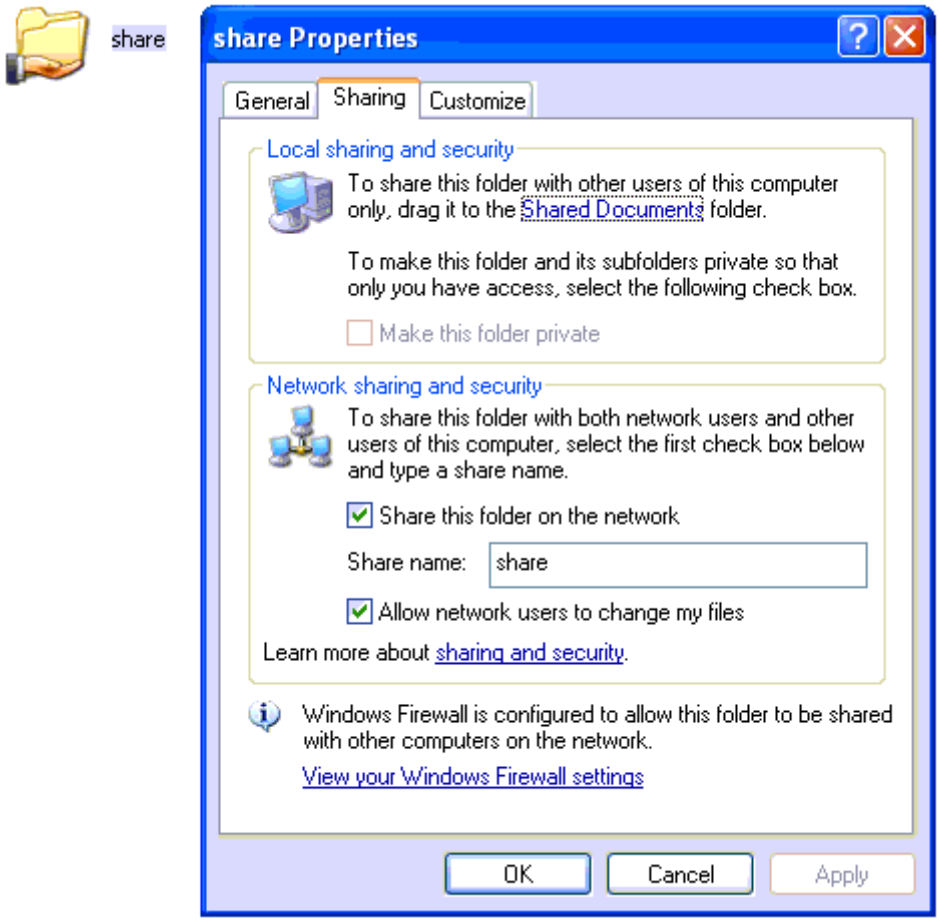

share
share Properties
General
Sharing
Customize
Local sharing and security
To share this folder with other users of this computer only, drag it to the Shared Documents folder.
To make this folder and its subfolders private so that only you have access, select the following check box.
Make this folder private
Network sharing and security
To share this folder with both network users and other users of this computer, select the first check box below and type a share name.
Share this folder on the network
Share name:
share
Allow network users to change my files
Learn more about sharing and security.
Windows Firewall is configured to allow this folder to be shared with other computers on the network.
View your Windows Firewall settings
OK
Cancel
Apply

Figure B-1 Set up share Properties

**Step 2**Enter the new folder and create a new text file, then rename this file to status.txt. This step is very important, DO NOT forget to create the status.txt file.

**Step 3**ConfigureAutobackup settings on mPBX to Figure B-2

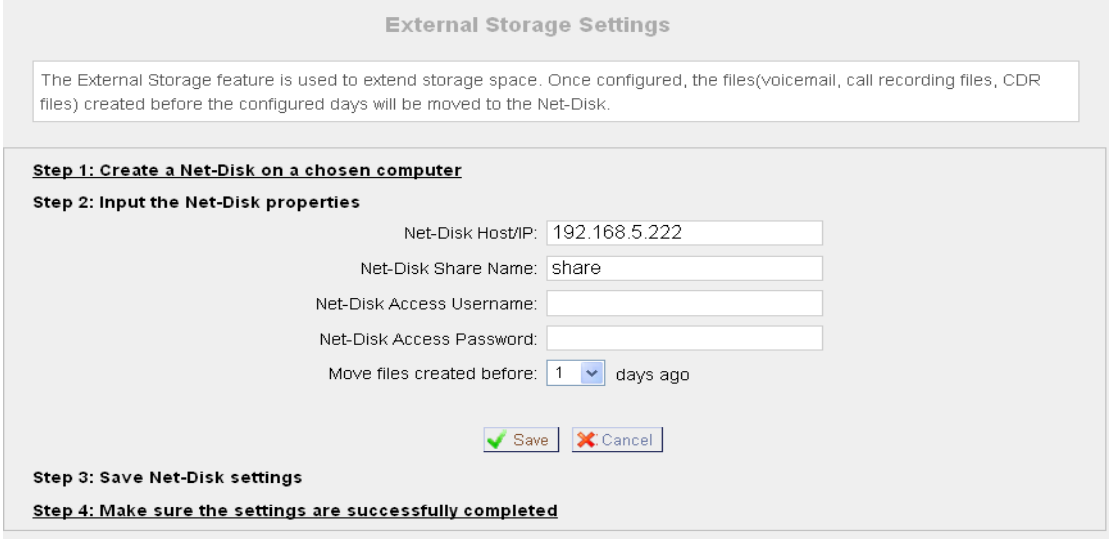

External Storage Settings
The External Storage feature is used to extend storage space. Once configured, the files(voicemail, call recording files, CDR files) created before the configured days will be moved to the Net-Disk.
Step 1: Create a Net-Disk on a chosen computer
Step 2: Input the Net-Disk properties
Net-Disk Host/IP: 192.168.5.222
Net-Disk Share Name: share
Net-Disk Access Username:
Net-Disk Access Password:
Move files created before: 1 days ago
Save
Cancel
Step 3: Save Net-Disk settings
Step 4: Make sure the settings are successfully completed

Figure B-2 Autobackup Setting

**Net-Disk Host/IP**:Change this to the IP address of the computer where backup files will be stored.

**Net-DiskShare Name**: Change this to the name of the shared folder where backups will be stored.

**Net-DiskShare Username**: The user name used to log into the network share. Leave this blank if it is not required

**Net-DiskShare Password**: The password used to log into the network share.Leave this blank if it is not required

If configuringis correctly, open your Windows share folder to see if the mPBX backup files and folders has been created.If the contents of the backup folder look similar to Figure B-3, then you have successfully configured Autobackup on the mPBX unit.

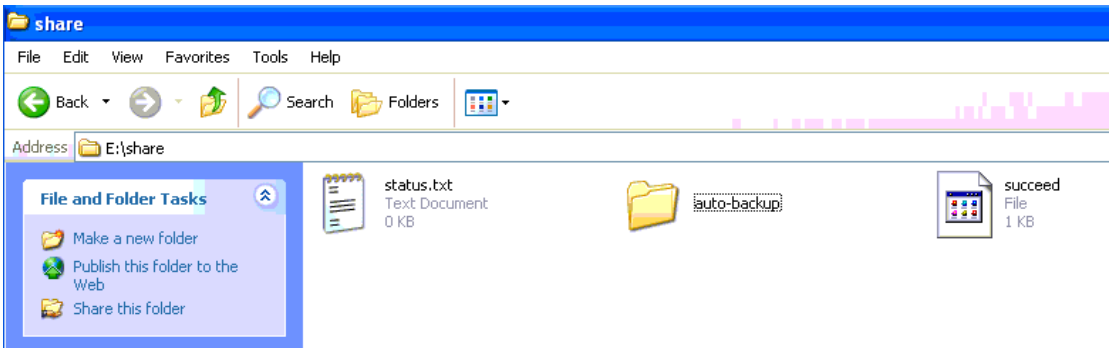



Figure B-3 Autobackup setting succeed

# APPENDIX C How to Configure NAT setting

**When mPBX is behind a NAT(firewall),you need to configure NAT setting on mPBX if you want to use a remote extension.**
Please follow section **1** or **2** below depending on your network configuration.
**1.** If mPBX is connected to a local network, you must set up port forwarding on your router. Specifically, you must map port 5060 (default SIP port) and port 10001-10200(default RTP port range) as UDP ports.

Next, go to the mPBX web interface and configurethe SIP settings according to Figure C-1:
**External IP Address**: your router's public IP address
**External Host**: your router's domain
**ExternalRefresh Interval**: 20 seconds
**Local Network Identification**:192.168.5.0/255.255.255.0 (change this according to your network configuration)
**NAT mode**: Yes
**Allow RTP Reinvite**: No

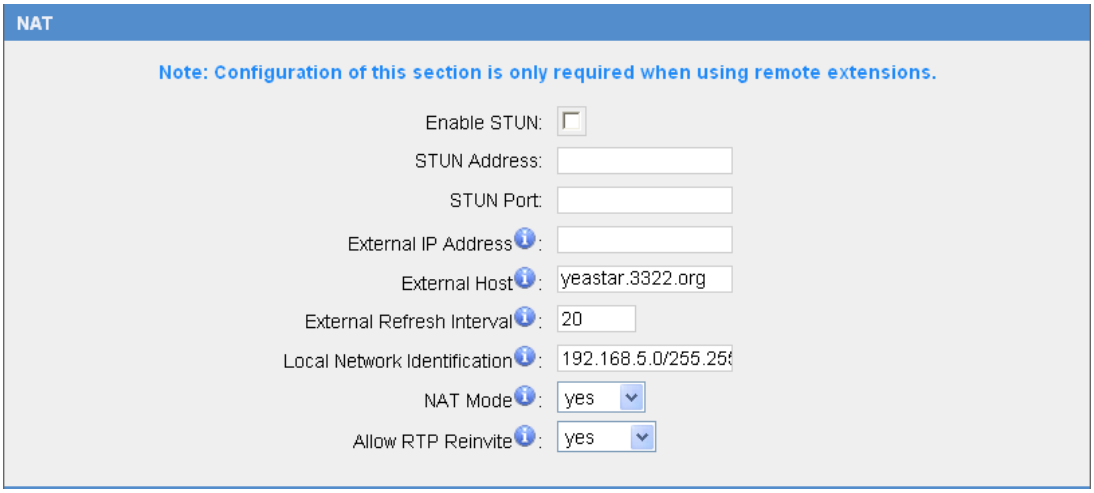



Figure C-1

Assuming that your router's host address is yeastar.3322.org, your local network is from 192.168.5.1-192.168.5.254, and the subnet Mask is 255.255.255.0, the mPBX network settings should configured like Figure C-2

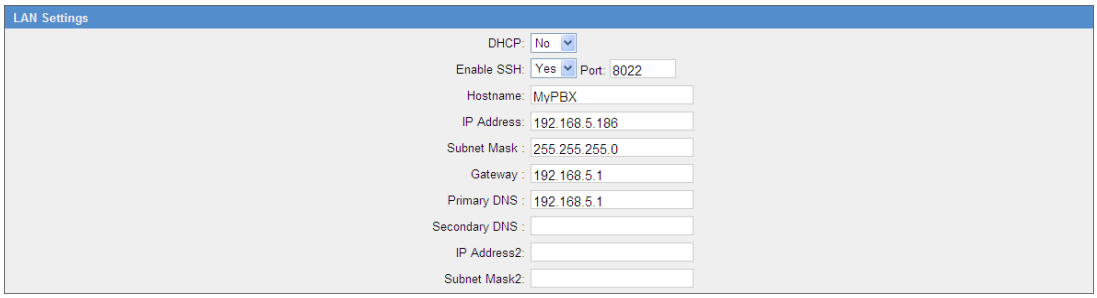



Figure C-2 mPBX Network setting

**2**. If mPBX has a public IP, (i.e. is connected directly to your internet service provider), the network settings should be configured according to Figure C-3:

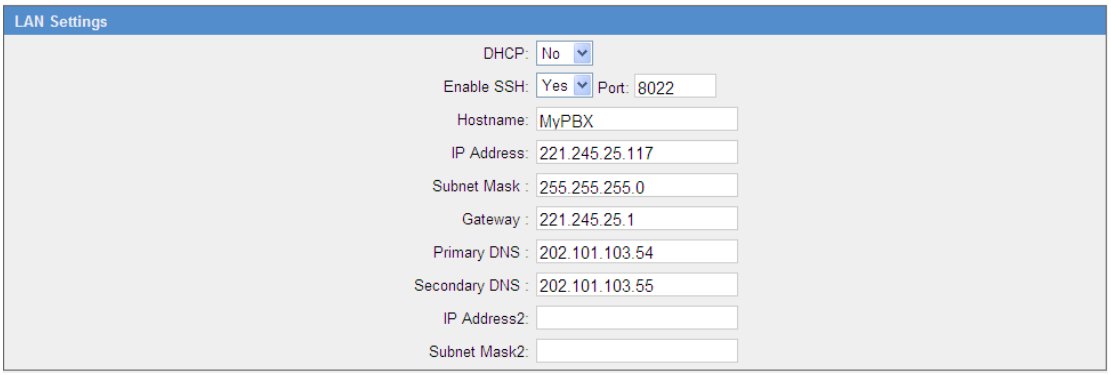



Figure C-3

Next, you should configure the NAT settingsaccording to Figure C-4

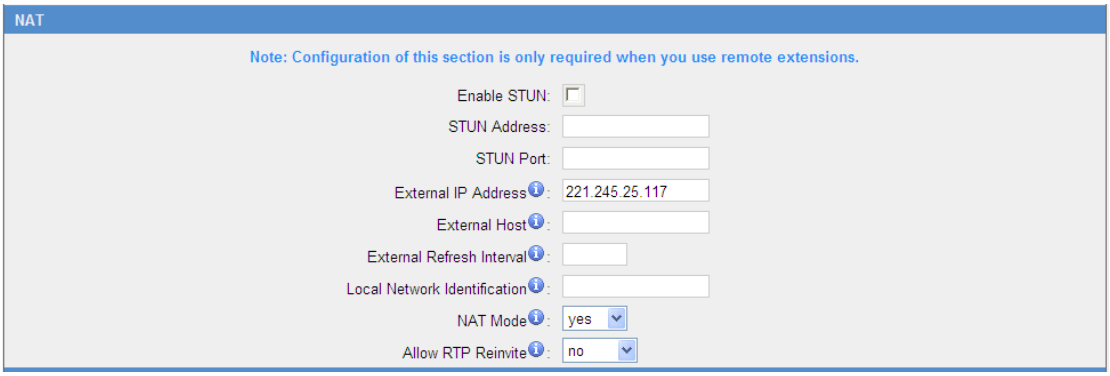



Figure C-4

**External IP Address**: The public IP address of mPBX
**External Host**: Leave this blank if no domain has been configured
**ExternalRefresh Interval**: Leave this blank
**Local Network Identification**: Leave this blank
**NAT mode**: Yes
**Allow RTP Reinvite**: No

# APPENDIX D How to Use Auto Provision

**Step1.** Disable DHCP Server on your local network.
E.g. Disable DHCP Server on Linksys Router.

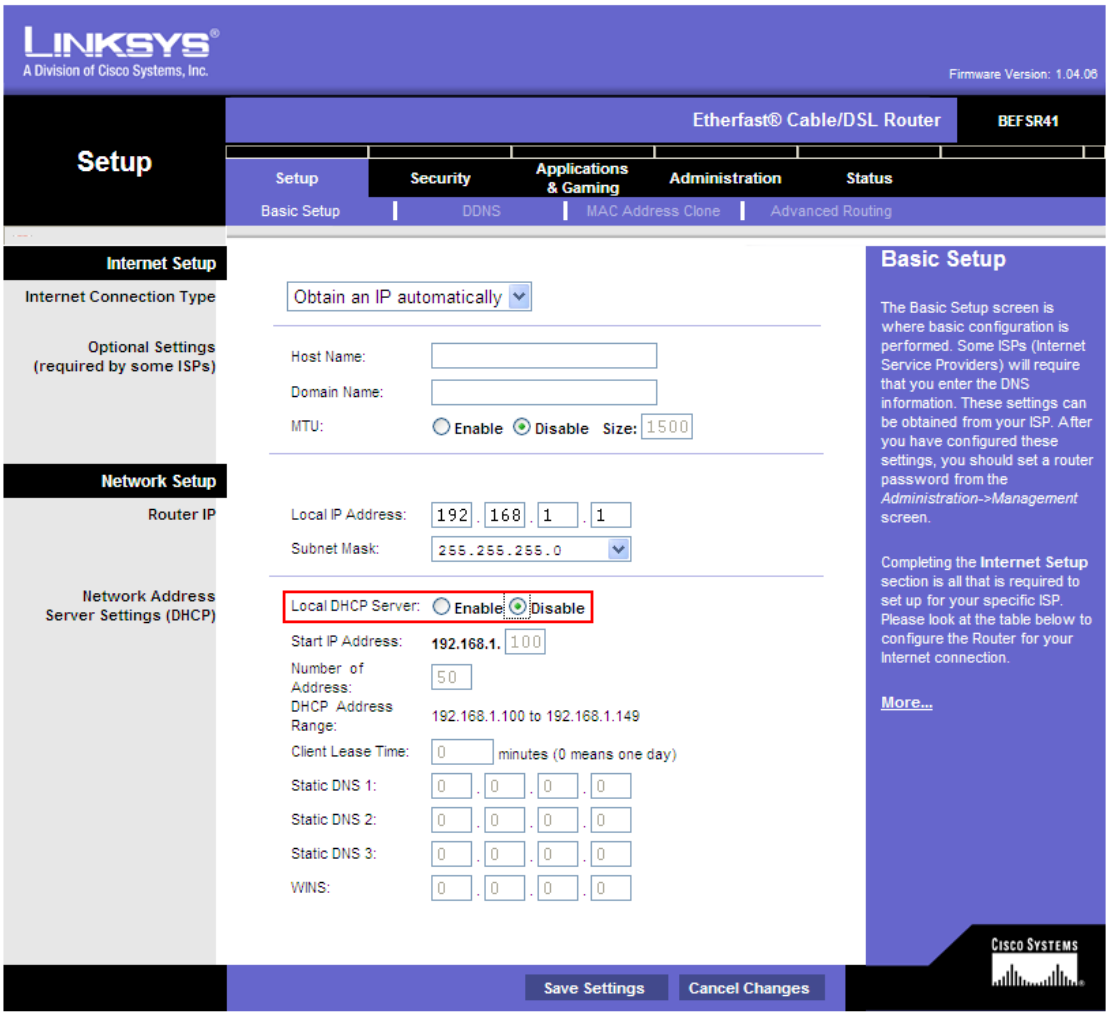



Figure D-1

**Step2.** Enable DHCP Server on mPBX.
Login mPBX web interface, System Settings → DHCP Server → Enable DHCP Server.

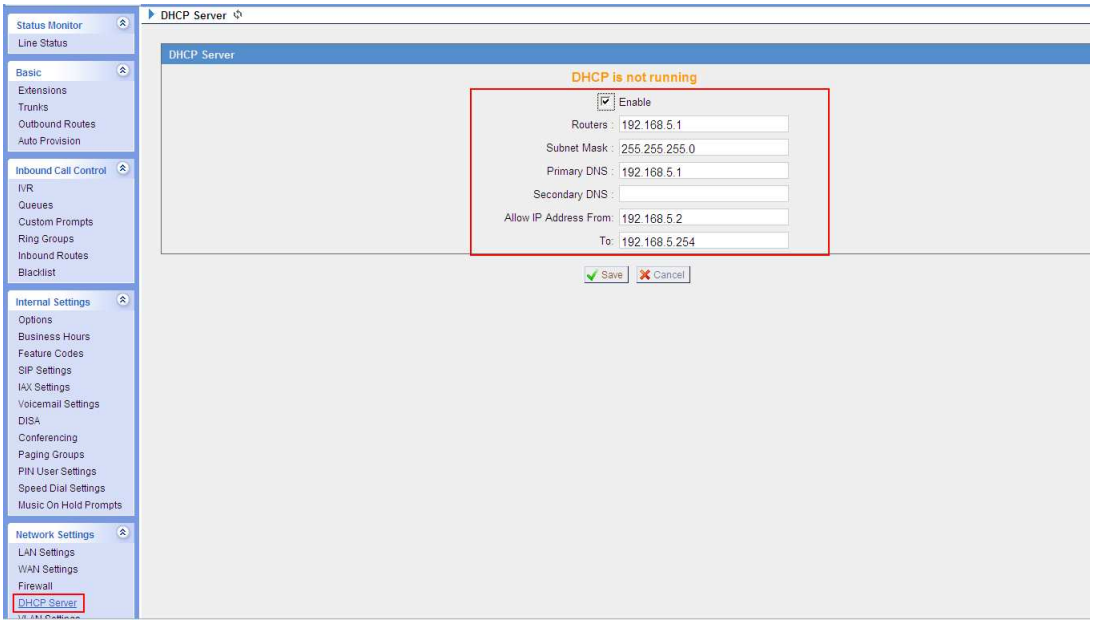



Figure D-2

**Step3.** Configure phones on mPBX auto-provision page.

1. Login mPBX web interface, Basic → Auto Provision → Create New Phone.

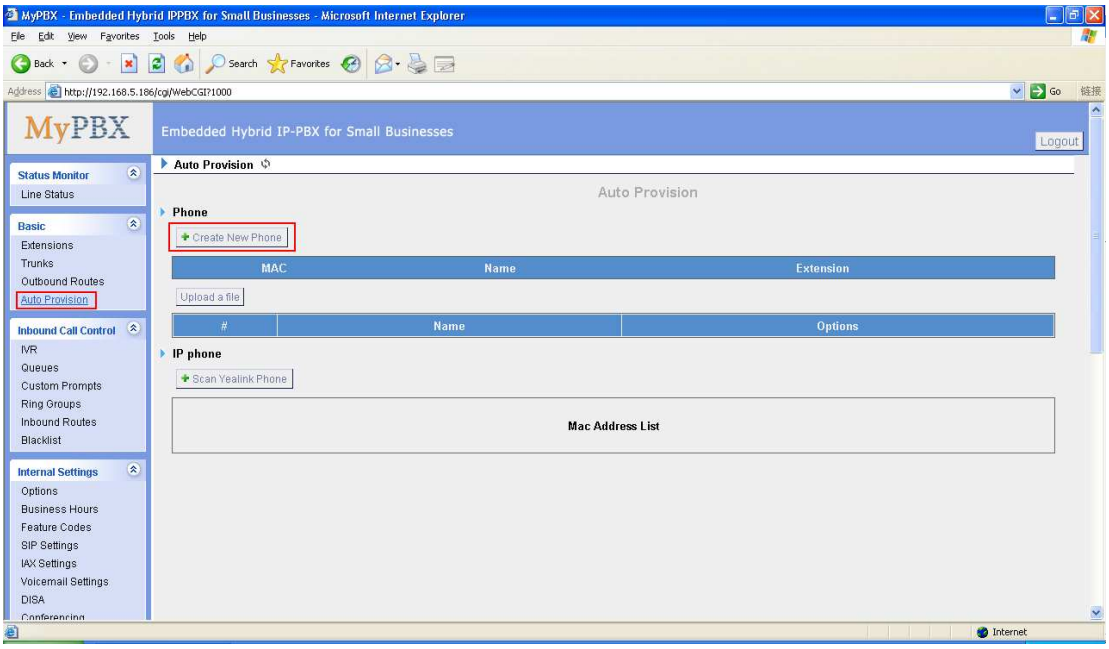



Figure D-3

2. Fill in the phone detail message on the pop-up windows.

Input IP Phone's MAC address, configure Name, Callwaiting, Line, Extension,Label, Line active for the phone.

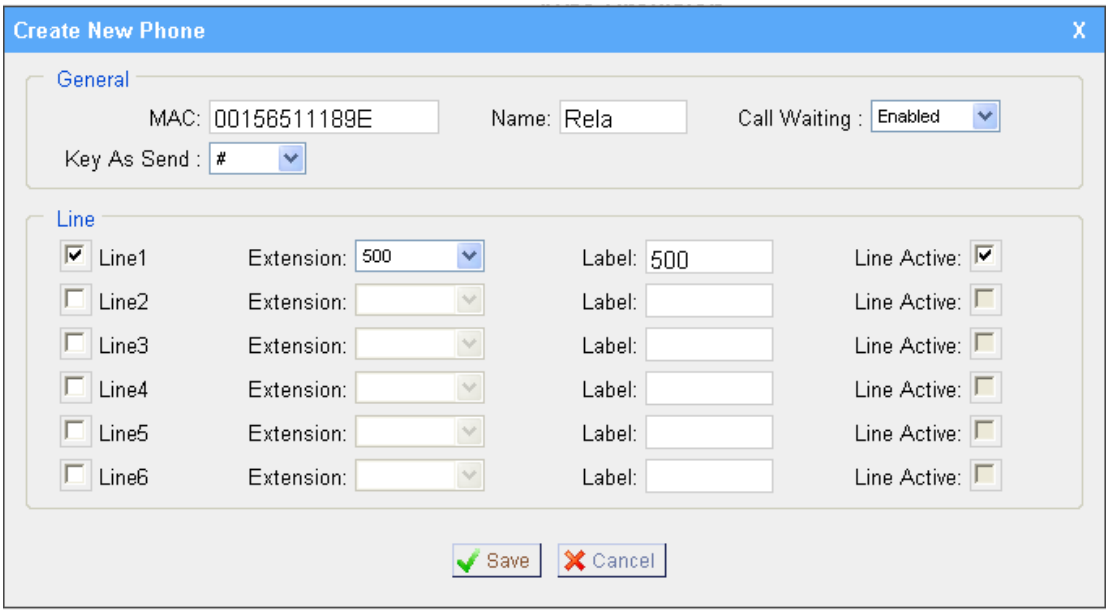



Figure D-4

**Step4.** Turn on the power and connect the network cable to IP Phone.
**Remark**: The factory default setting of DHCP for IP Phone is enable, so you can skip this step to step 5.
If the DHCP is disable, please follow below step to enable it. (e.g.: Yealink's IP Phone).
1. Login IP phone's web page.
2. Enable DHCP.

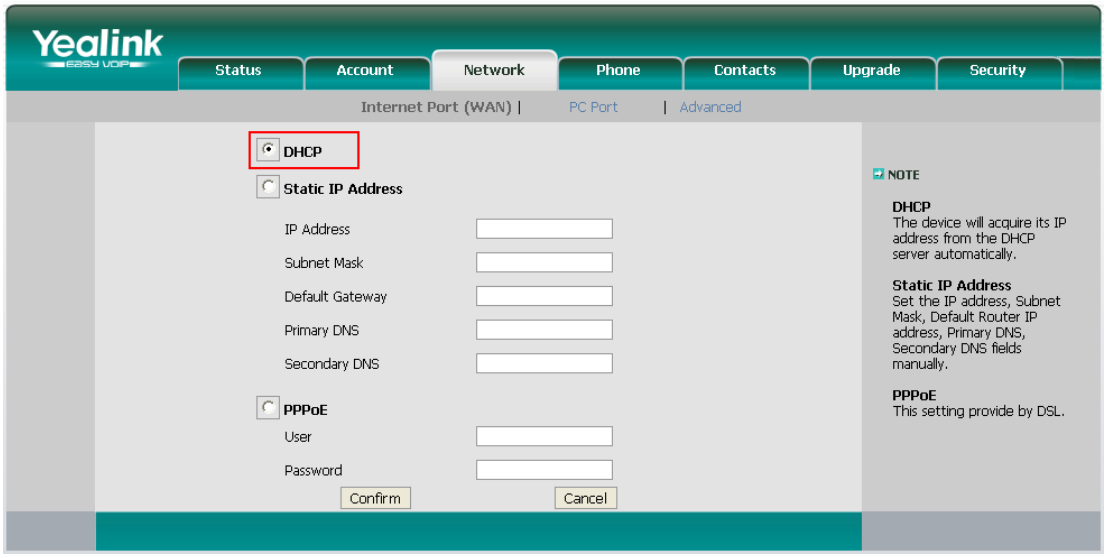
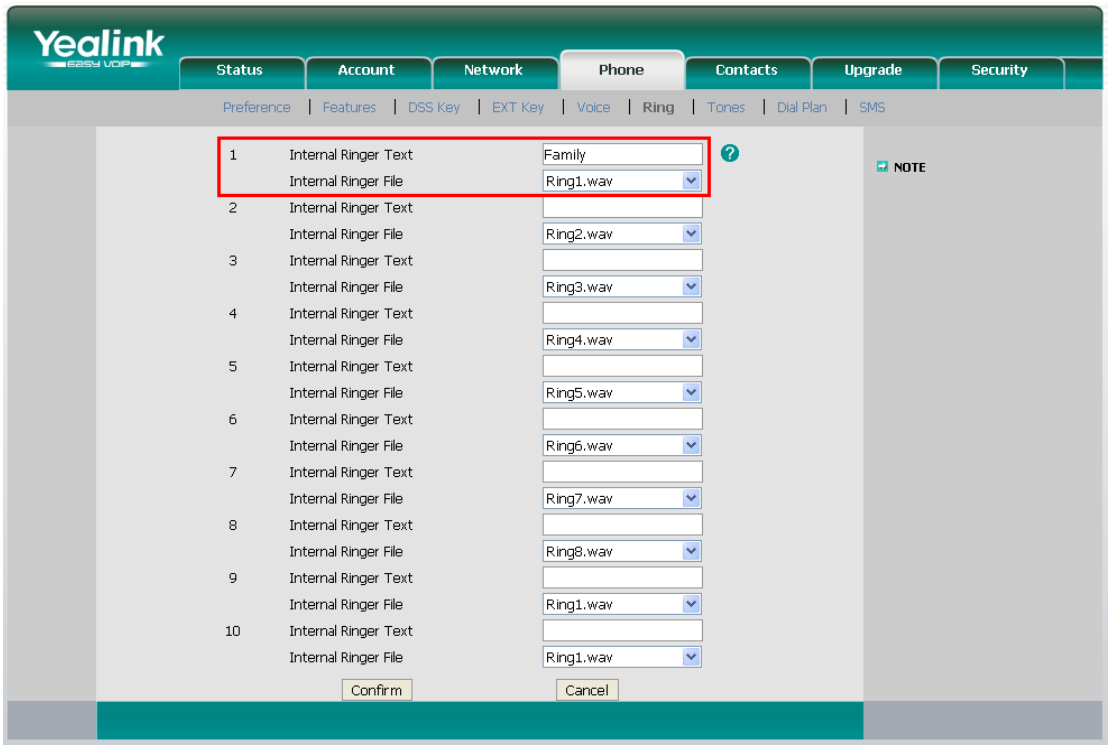



Figure D-5

**Step5.** Finish.

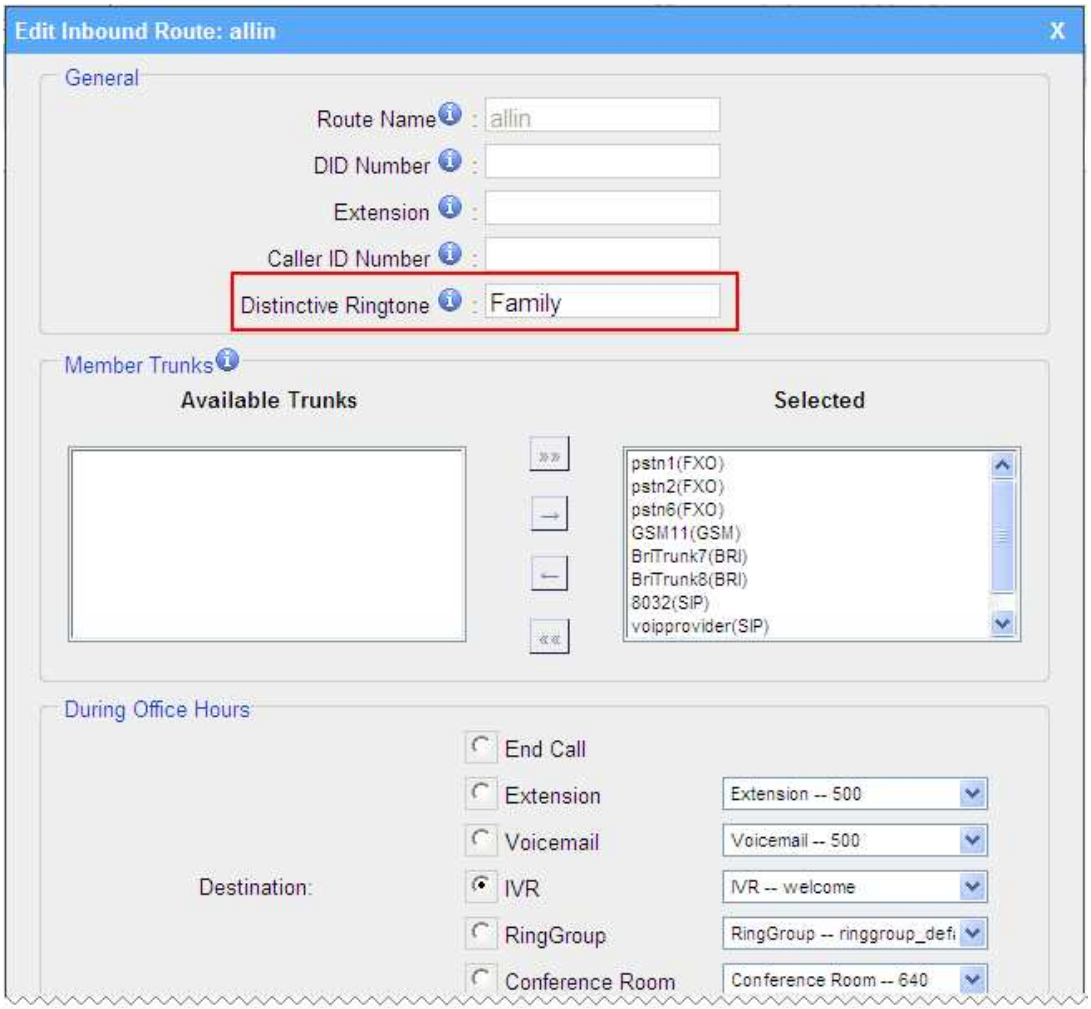
# APPENDIX E HowDo I Configure Distinctive Ring Tones

**Step1**: On your IP phone, navigate to the Phone settings web configuration page and find the Distinctive Ring Tone section.
For each custom ring tone, enter the Internal Ringer Text (can be digits or text) to trigger the ring tone. For example, you may enter "Family".
e.g.: Yealink's IP phone.




FigureE-1

**Step2.**Configure the 'Distinctive Ringtone' on mPBX.
mPBX web interface, Inbound Routes →Edit Inbound Route, fill in the Internal Ringer Text on 'Distinctive Ringtone'.




FigureE-2

**Step3.** Finish.

# APPENDIX F How to Use DID

Direct inward dialing (DID), also called direct dial-in (DDI) in Europe and Oceania, is a feature offered by telephone companies for use with their customers' private branch exchange (PBX) systems. In DID service the telephone company provides one or more trunk lines to the customer for connection to the customer's PBX and allocates a range of telephone numbers to this line (or group of lines) and forwards all calls to such numbers via the trunk.

mPBX support DID, you can configure DID in inbound route. Related settings: **DID Number, Extension, Destination.**

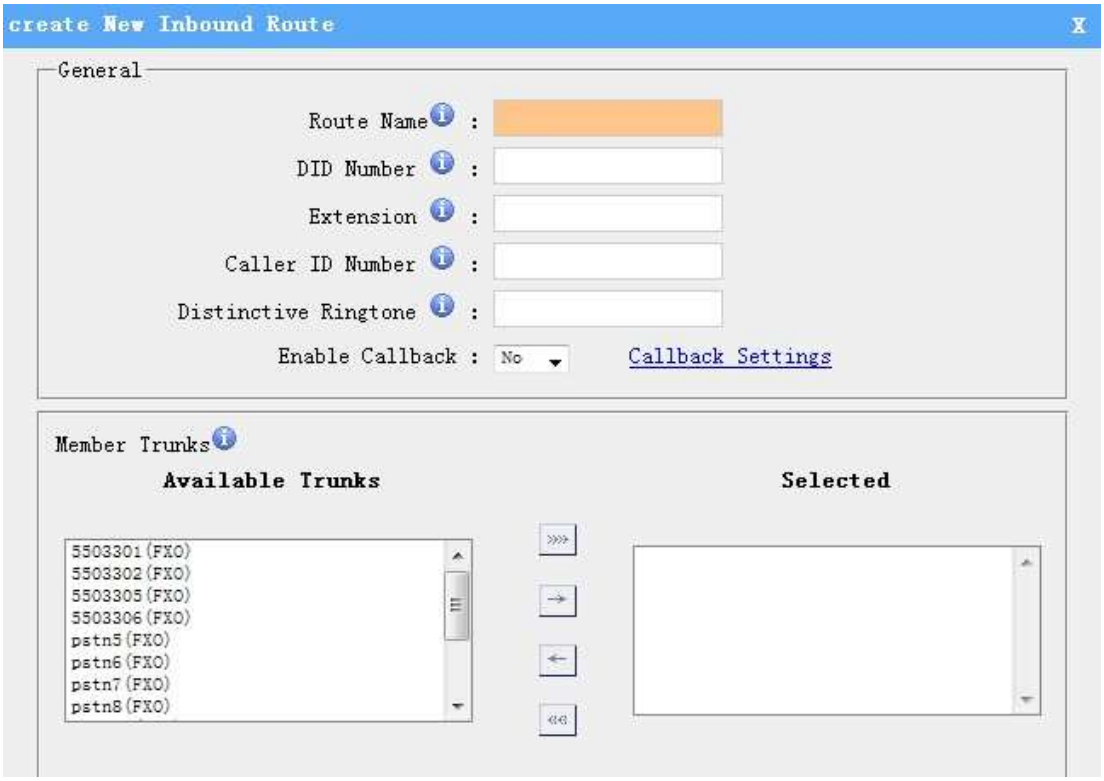



Figure F-1

**·DID Number**

Define the expected DID Number if this trunk passes DID on incoming calls. Leave this field blank to match calls with any or no DID info. Only service provider, E1 trunks, BRI trunks or SIP trunks need to be configured with this setting.

You can also use pattern matching to match a range of numbers.The following patterns may be used:

**X**: Any Digit from 0-9
**Z**: Any Digit from 1-9
**N**: Any Digit from 2-9
**[12345-9]**: Any digit in the brackets (in this example, 1,2,3,4,5,6,7,8,9)
The '**.**'Character will match any remaining digits. For example, 9011. will match any phone number that starts with 9011, excluding 9011 itself.
The '**!**' will match none remaining digits, and causes the matching process to complete as soon as it can be determined that no other matches are possible.

**·Extension**
Define the extension for DID number, this field only valid when use E1 trunk for this inbound router.You can only input number and '-' in this field, and the format can be xxx or xxx-xxx.The count of the number must be only one or equal the count of the DID number.

**·Destination**
If you don't set the extension, you can set the destination of the call here.

**Example 1:**
Step1: You set the DID number (5503XXX in this example).
Step2: You choose the destination(Ring Group in this example).

The configuration of this example means when the incoming call with DID number 5503XXX (7 digits number start with 5503) will go to the destination Ring Group.

If you choose the destination, please leave the Extension form blank.

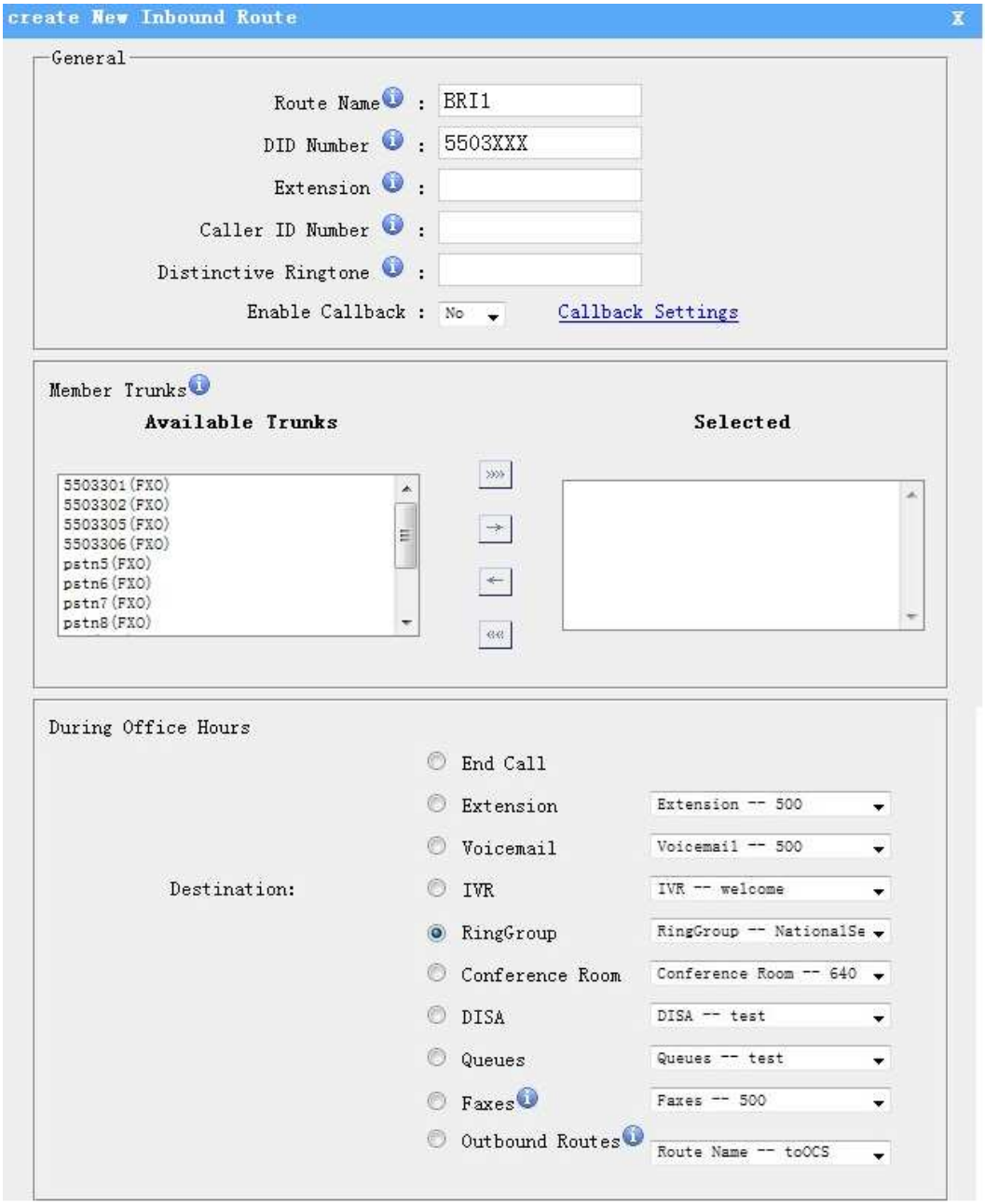



Figure F-2

**Example 2:**

Step1: You set the DID number (6001-6099 in this example).

Step2: You set the Extension (6001-6099 in this example).

The configuration of this example means when the incoming call with DID number 6001 to 6099 will go to the destination 6001 to 6099(number 6001 to extension 6001, number 6002 to extension 6002).

The destination you set below will be disabled if you set the Extension.

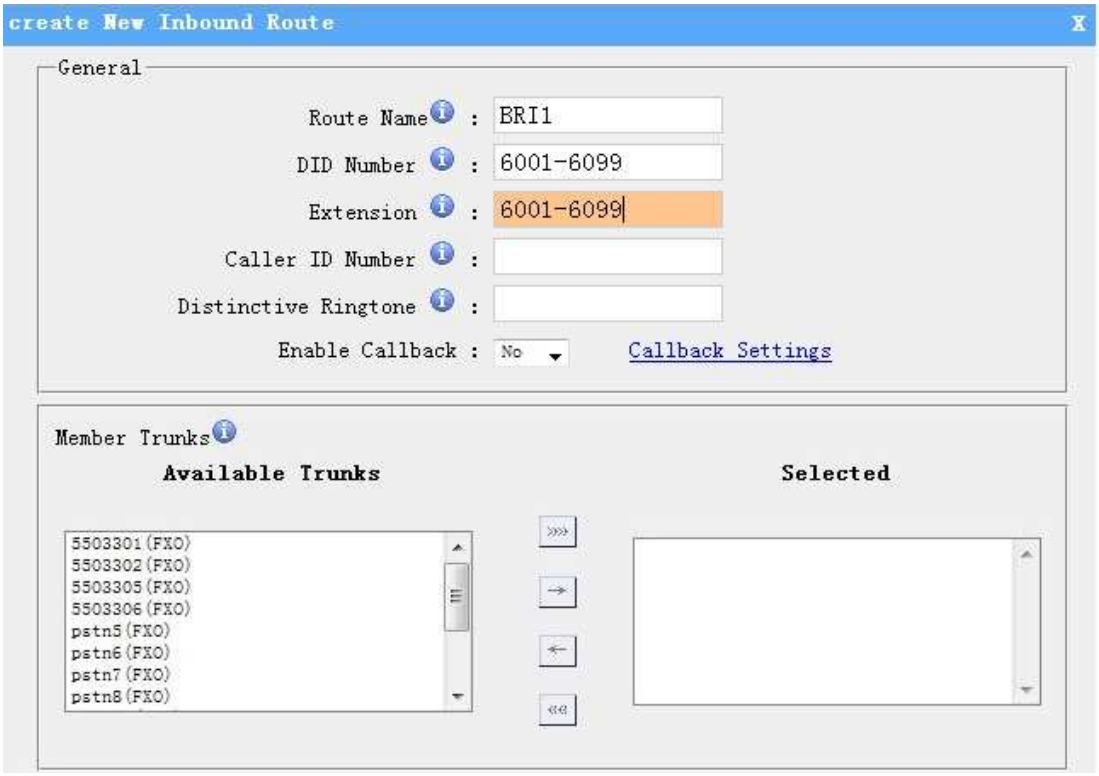

create New Inbound Route
X
General
Route Name : BRI1
DID Number : 6001-6099
Extension : 6001-6099
Caller ID Number :
Distinctive Ringtone :
Enable Callback : No
Callback Settings
Member Trunks
Available Trunks
Selected
5503301(FXO)
5503302(FXO)
5503305(FXO)
5503306(FXO)
pstn5(FXO)
pstn6(FXO)
pstn7(FXO)
pstn8(FXO)

Figure F-3

# APPENDIX G mPBX Security configuration Guide

VoIP attacks, although it is not an everyday occurrence, it does exist. While using VoIP, system security is undoubtedly one of the issues we care about most. But with the appropriate configuration, and some basic safety habits, we can improve the security of the telephone system. Moreover, the powerful built-in firewall function in mPBX is adequate to enable the system to run safely and stably.
This guide will introduce the highest defense level in mPBX, and we strongly recommend that you configure firewall and other security options according to this guide, to prevent the attack fraud and the system failure or calls loss.

**Note**: In this guide, the configuration options marked with '*' only exist in 12.17.XX.XX and above versions, namely, 3.2 guest calls option, 3.3 remote registered option, and 5 alarm settings.

## 1. Security Configuration for Web GUI

### 1.1 Change the default access port for HTTP on Options page

PBX→Basic Settings→General Preferences→HTTP Bind Port

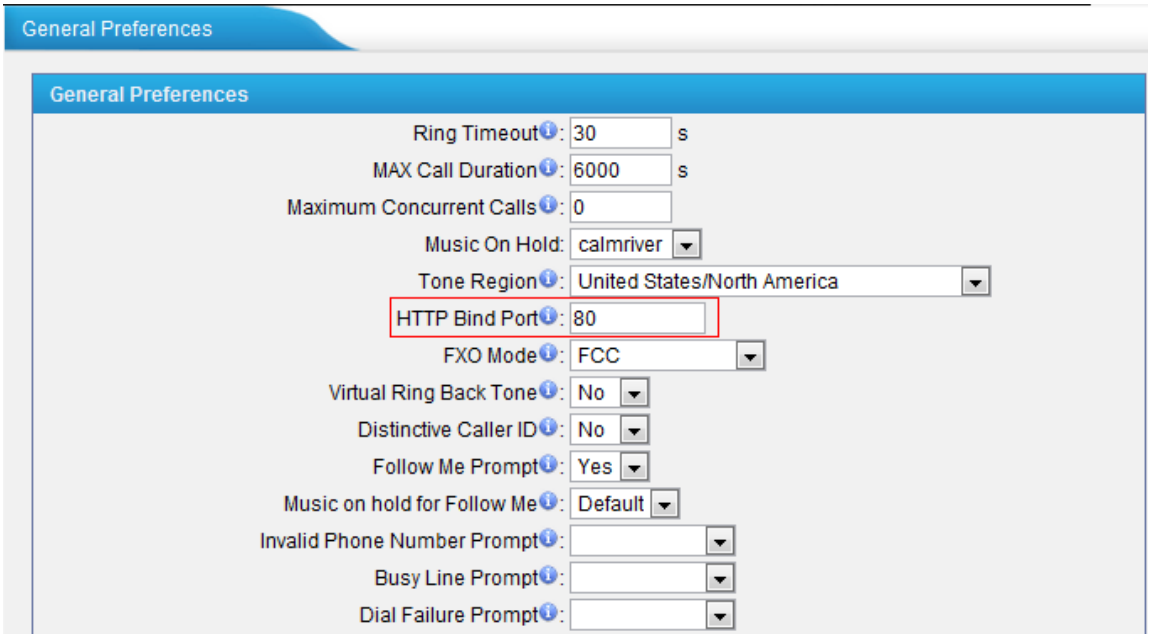
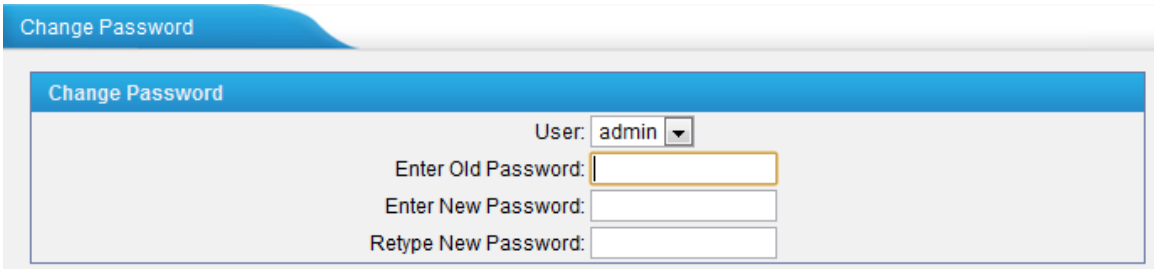



Figure G-1

## 1.2 Change the default password for the web GUI

System→System Preferences→Change Password




FigureG-2

# 2. Disable SSH on LAN Settings Page

## 2.1 Disable SSH

Select LAN Settings→Enable SSH. If external debugging isn't required, please select "No".

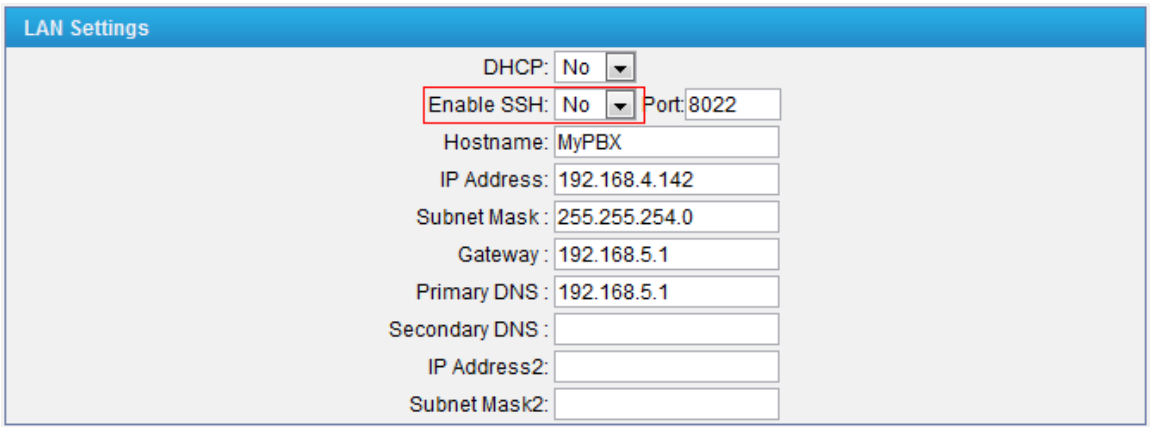



Figure G-3

## 2.2 Change the default password for SSH

We can use the Linux command passwd to change root password of mPBX.

1. Login via putty.exe

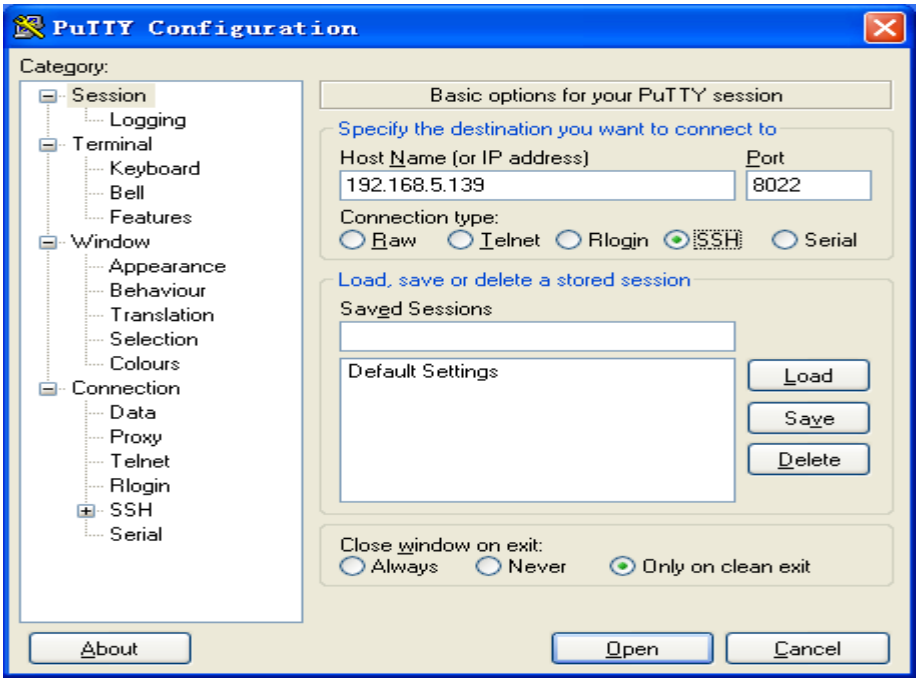



Figure G-4

2. The default username is root and the default password is ys123456.

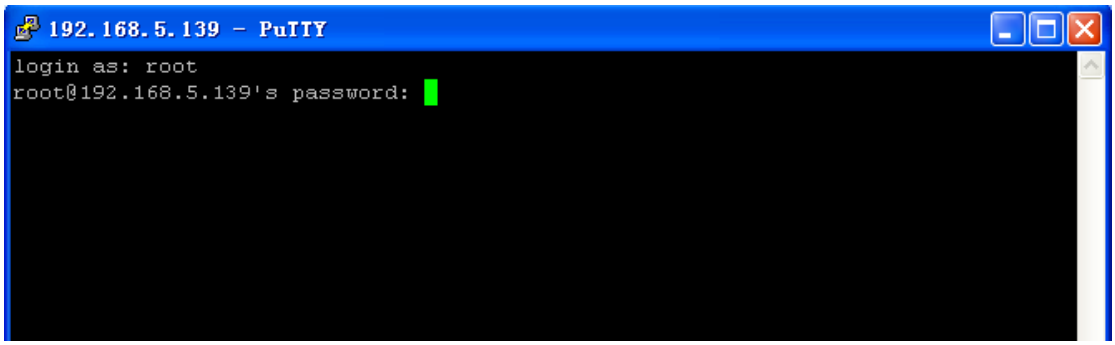



Figure G-5

3. Step 2 use command passwd to change the root's password

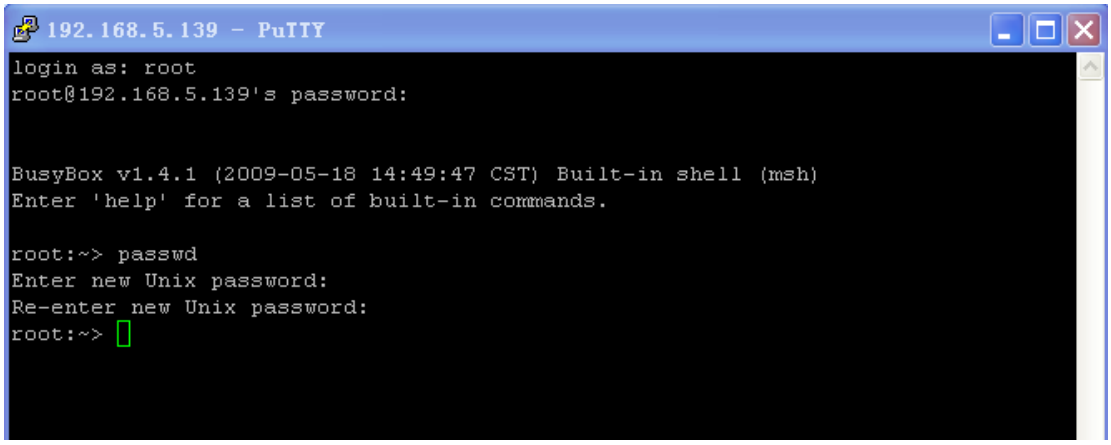



Figure G-6

# 3. Security Configuration for Extensions

## 3.1 Change the default SIP Port

PBX→Basic settings→SIP Settings→General→UDP Port

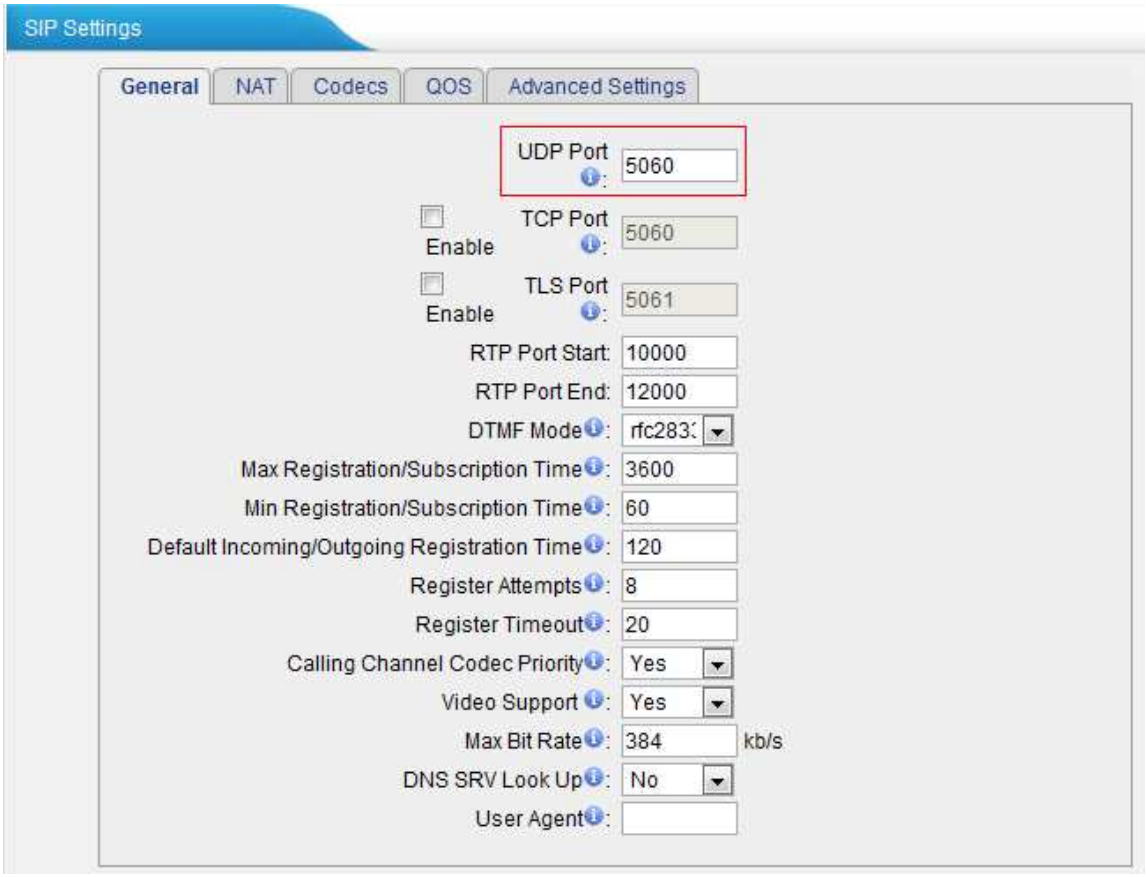



Figure G-7

## 3.2*Disable guest calls

PBX→Basic settings→SIP Settings→Advanced Settings→Allow Guest

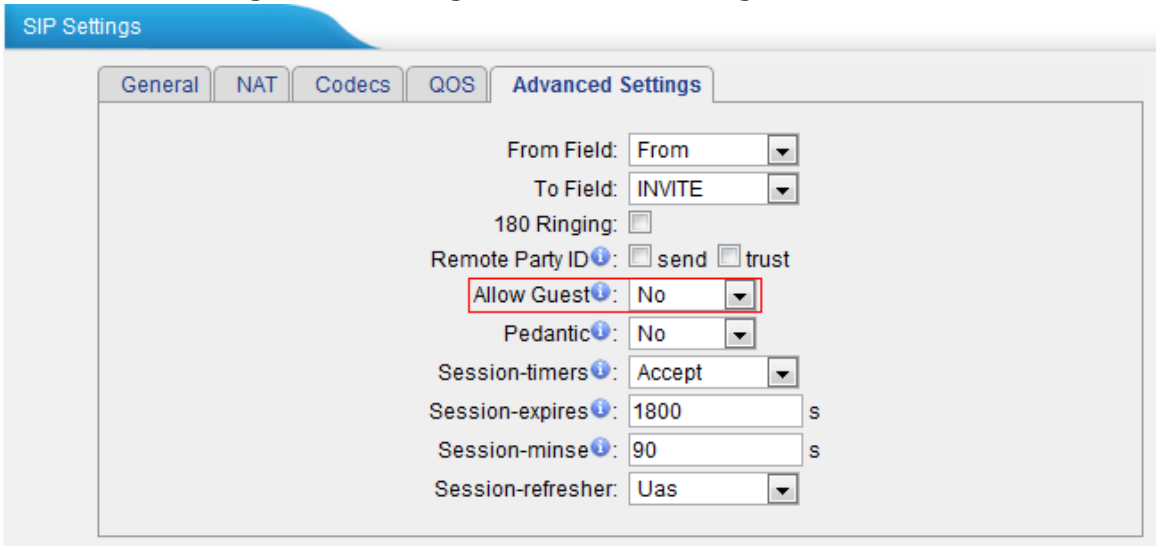



Figure G-8

## 3.3* Security Configuration for remote extensions

If remote registration isn't required, please disable it.
PBX→Extensions→FXS/VoIP Extensions→VoIP Extensions→General→VoIP Settings

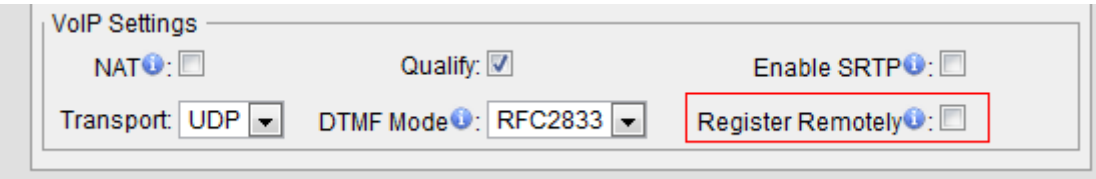



Figure G-9

## 3.4 Set an enhanced password and enable IP restriction for extensions

1) Set a new extension password at the higher security level, e.g. AjK5Up1G.

PBX→Extensions→FXS/VoIP Extensions→VoIP Extensions→General→Password

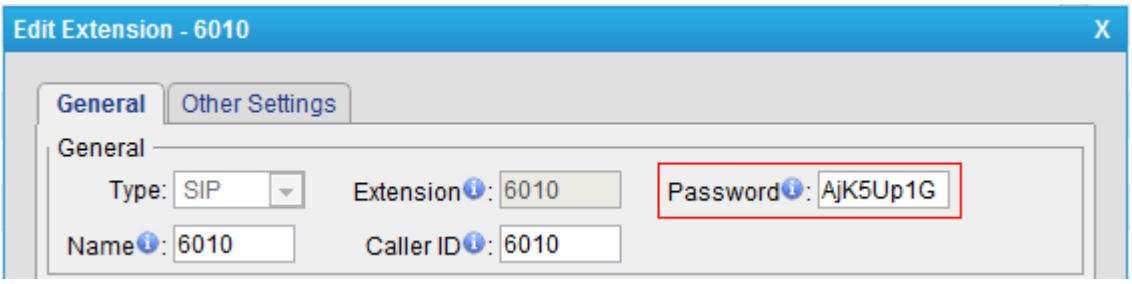



Figure G-10

2) Enable IP restriction and enter the permitted "IP address/Subnet mask", e.g. 192.168.5.136.

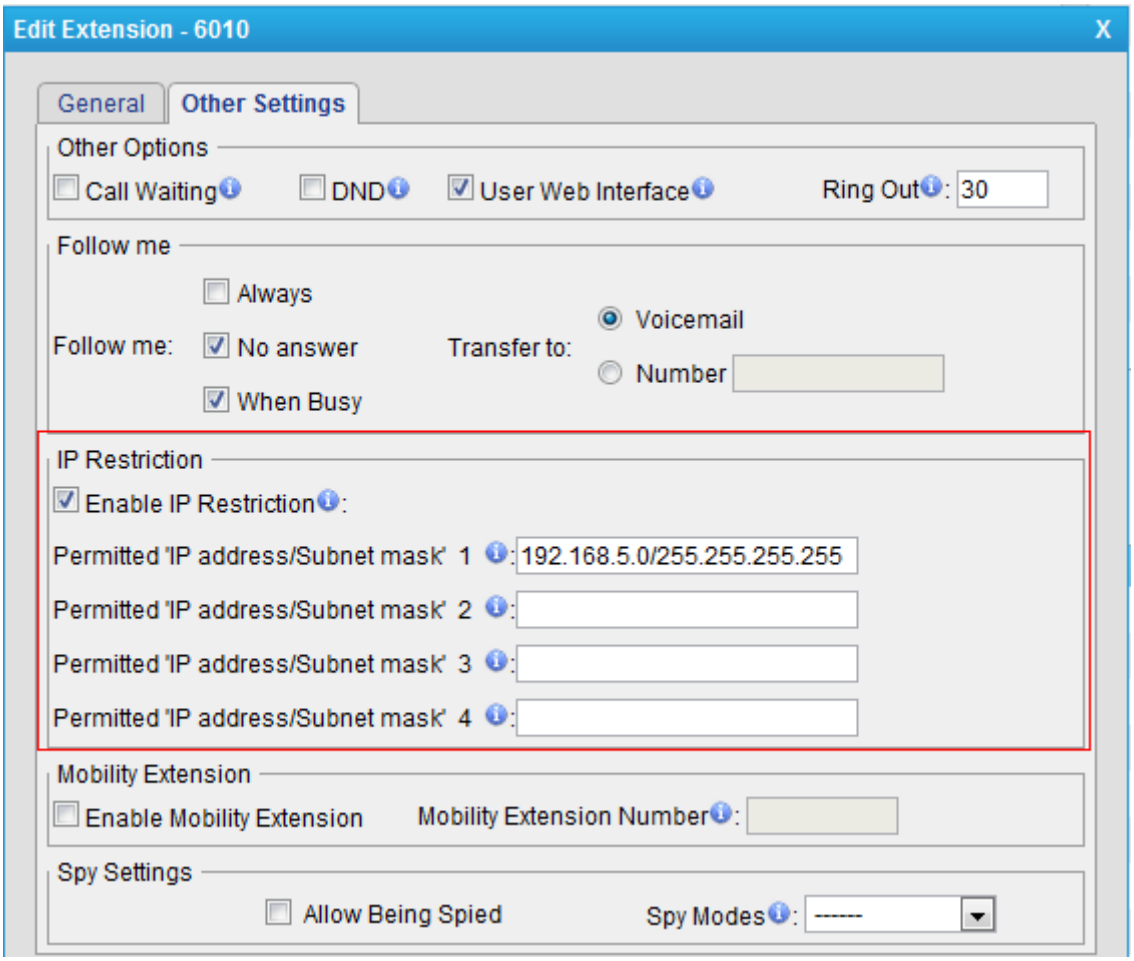



Figure G-11

# 4. Setup Proper Firewall Rules

**Note**: Please backup the configurations on backup and restore page before you go ahead.In the case that you lock the device, you can reset to factory default and restore the previous configurations. Below example rules works with mPBX firmwareversion 2.15.xx.xx or higher versions.

**Step1**. Enable firewall on firewall page of mPBX.
System→Firewall Settings→Firewall Rules→General Settings

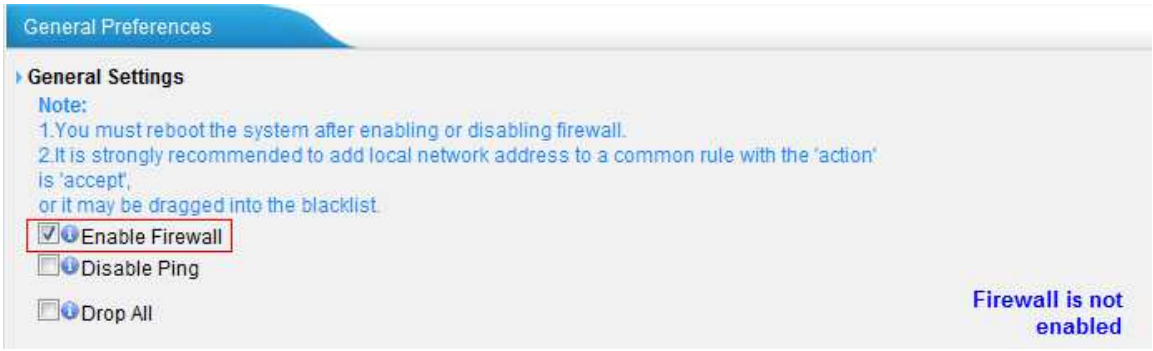

General Preferences
General Settings
Note:
1.You must reboot the system after enabling or disabling firewall.
2.It is strongly recommended to add local network address to a common rule with the 'action' is 'accept',
or it may be dragged into the blacklist.
Enable Firewall
Disable Ping
Drop All
Firewall is not enabled

Figure G-12

**Step2**.Add a common rule to accept local network access.

Create a common rule to allow the all the IP addresses of the local phones to access mPBX server. For example, if the IP addresses of the local network are 192.168.5.1-254, the configurations could be as below:

**Name**: LocalNetwork

**Protocol**: BOTH

**Port**: 1:65535

**IP**: 192.168.5.0/255.255.255.0

**Action**: Accept

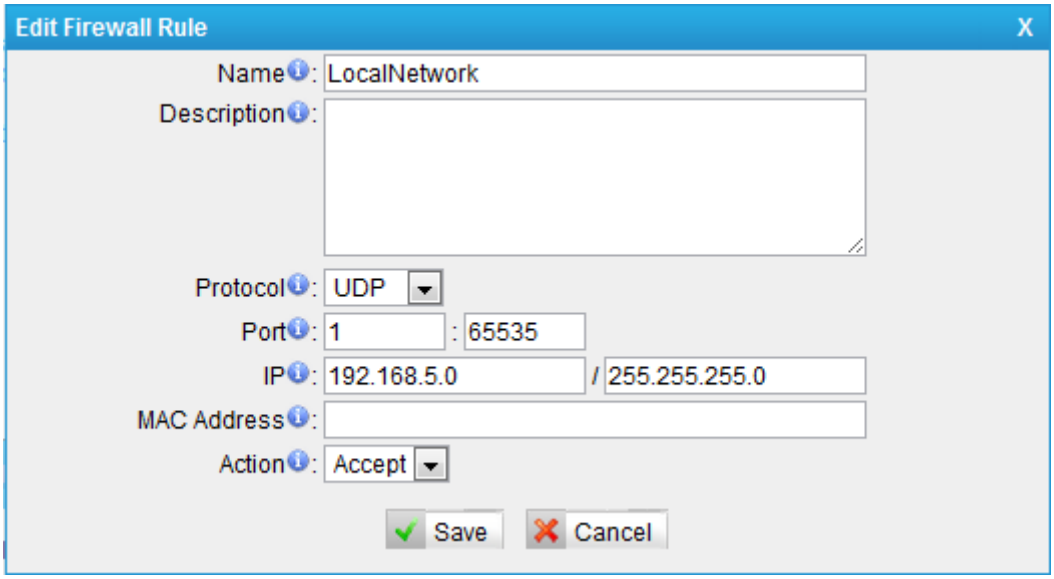



Figure G-13

**Step3**. Create common rules to accept remote extensions or remote administrators, if you use SIP trunk, please accept the provider's host as well.

**Note**: If there are no remote extensions, the rule is not required.

1) Set up the firewall rule to allow the public IP address of remote extensions to access mPBX server. e.g.110.111.132.6, the configurations could be as below:

   **Name**: Remote Extension

   **Protocol**: BOTH

   **Port**: 1:65535

   **IP**: 110.111.132.6/255.255.255.255

   **Action**: Accept

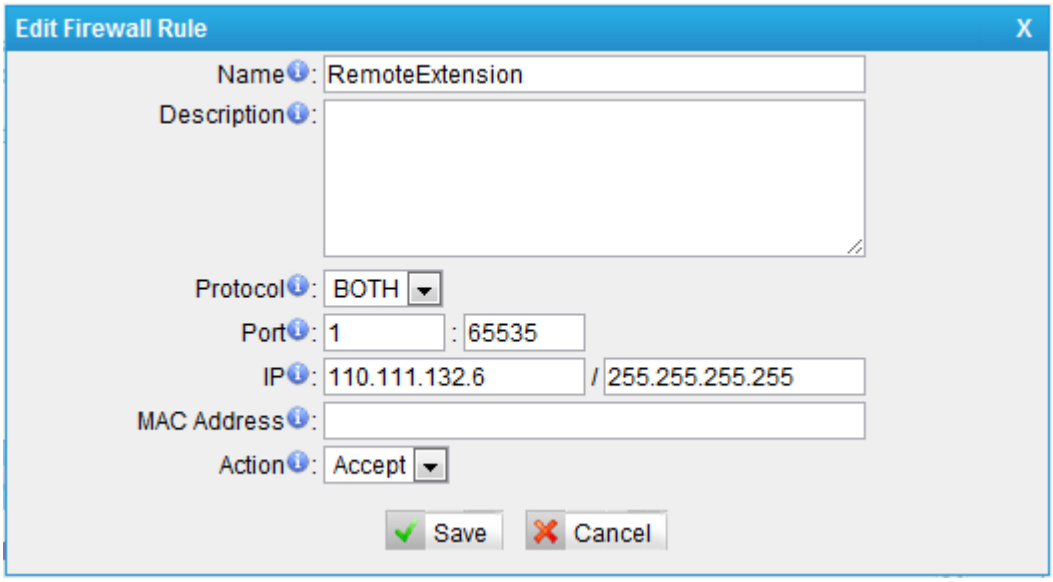



Figure G-14

**Step4**.Configure auto blacklist rules

Auto blacklist rules: the Server would add the IP address to the blacklist automatically if the number of the packets it sends exceed the rule you configured.

1) Add two auto blacklist rules for port: 5060.

Rule No.1:

**Port**: 5060

**Protocol**: UDP

**IP Packets**: 120

**Time Interval**: 60 seconds

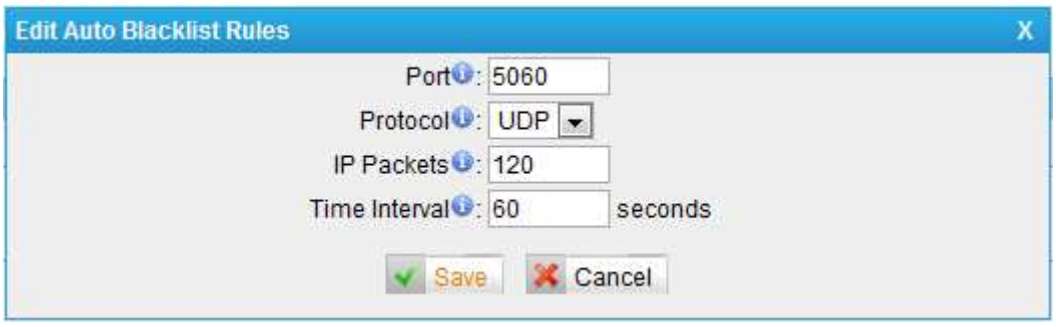



Figure G-15

Rule No.2:

**Port**: 5060

**Protocol**:UDP

**IP Packets**: 40

**Time Interval**: 2 seconds

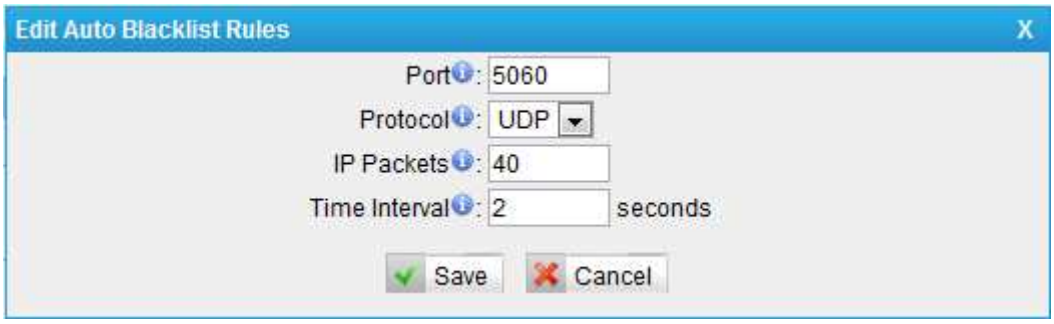



Figure G-16

2) Add an auto blacklist rule for Port:8022

Rule No.3

**Port**:8022

**Protocol**: TCP

**IP Packets**: 5

**Time Interval**: 60 seconds

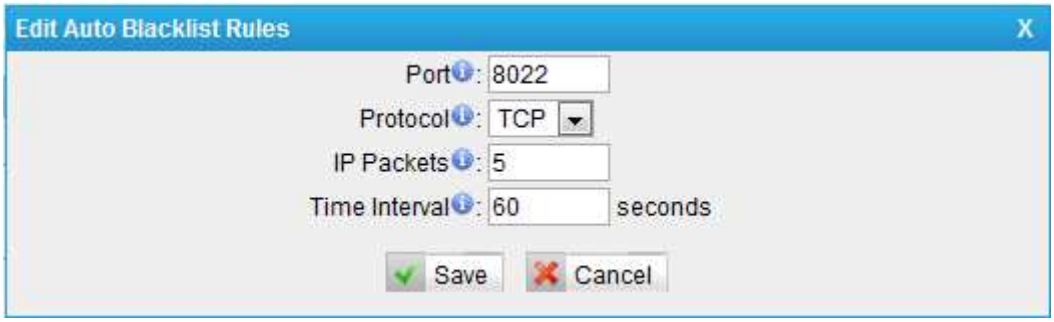



Figure G-17

**Step 5**. Add a Firewall Rule for VoIP trunk registration

**Note**: If there is no VoIP trunk, this rule is not required. And if the RTP IP address of VoIP trunk and Registration IP address of the VoIP trunk are different, we need create a rule to accept the RTP IP address too.

Add a rule to accept the IP address of the VoIP trunk to access mPBX server. For example: If the IP address of the VoIP trunk is 110.5.14.6, Protocol is UDP and Port is 5060, the configuration could be as below:

**Name**: VoIPTrunk

**Protocol**: UDP

**Port**: 5060: 5060

**IP**: 110.5.14.6/255.255.255.255

**Action**: Accept

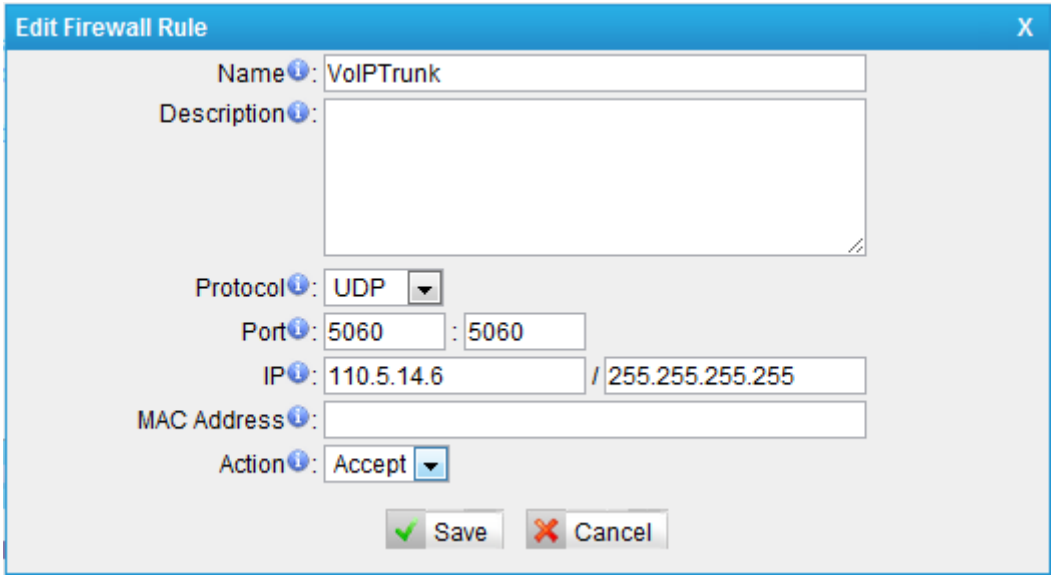



Figure G-18

**Step6**. Add a firewall rule to accept the remote access of HTTP port. For example, if the remote access IP is 110.5.14.6, and the port is 80, the configuration could be as below.

**Name**: RemoteHTTP
**Protocol**: TCP
**Port**: 80:80
**IP**: 110.5.14.6/255.255.255.255
**Action**: Accept

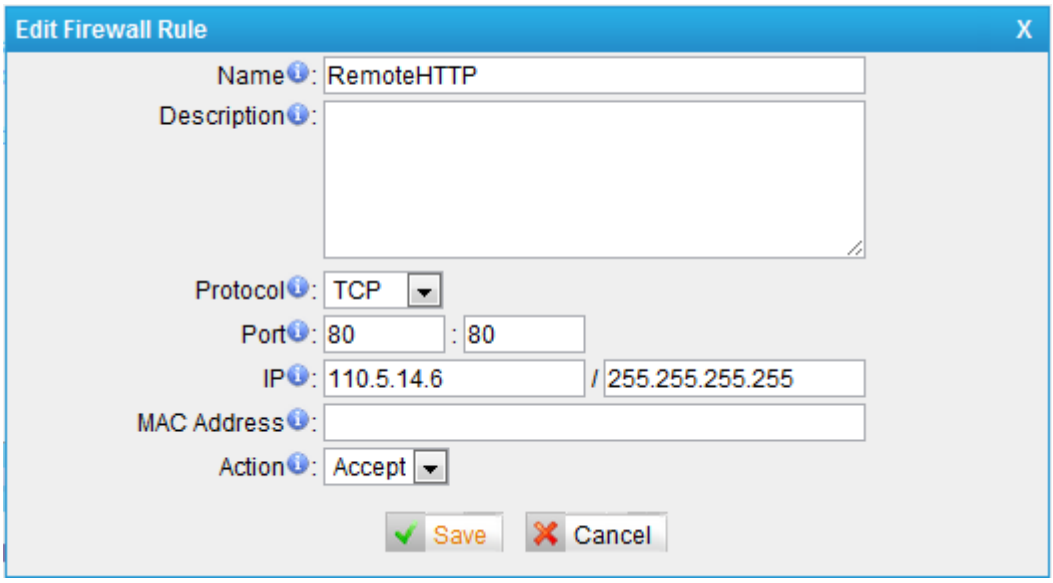



Figure G-19

**Step 7**. Add a firewall rule to accept remote access of SSH port. For example: if the remote access IP is 110.5.14.6 and the port is 8022.

**Note**: If the remote access of SSH port is not needed, this rule is not required.

**Name**: RemoteSSH
**Protocol**: TCP
**Port**: 8022:8022
**IP**: 110.5.14.6/255.255.255.255
**Action**: Accept

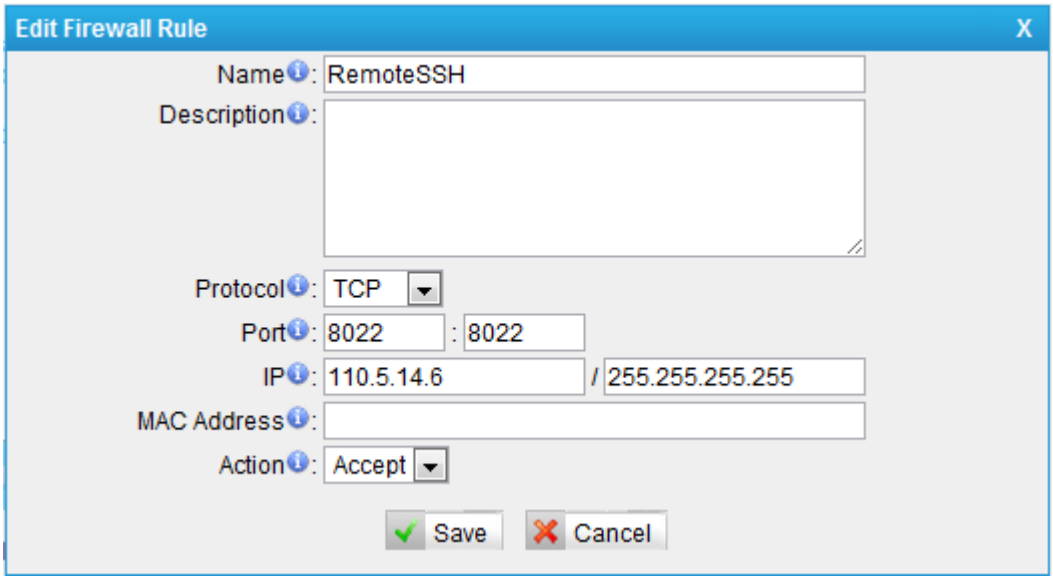



Figure G-20

**Step 8**. Add other firewall rules by yourself. For example, if you are using features about email, you should add the firewall rules for the SMTP server and POP3 server.

**Step 9**. Enable Drop all (If this feature is enabled, all the packets and connection that do not match the rules would be dropped.)

**Note**: Before enable this feature, please add a rule to accept the local network access, or the server might not be accessed.

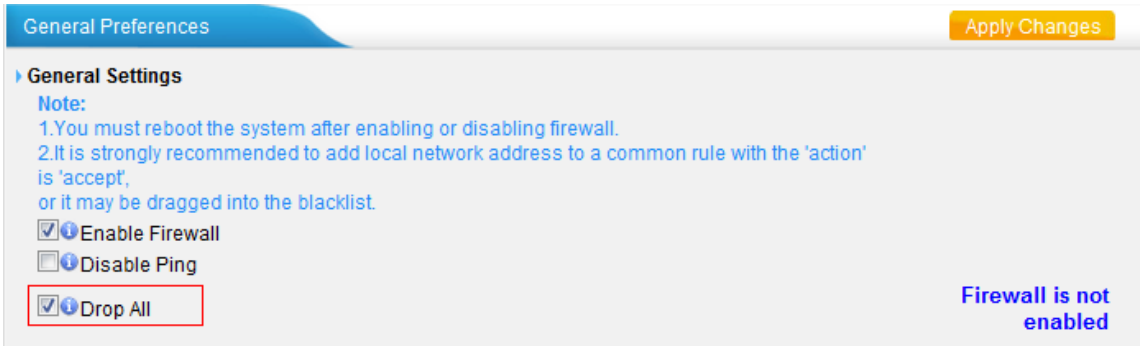

General Preferences
Apply Changes
General Settings
Note:
1.You must reboot the system after enabling or disabling firewall.
2.It is strongly recommended to add local network address to a common rule with the 'action' is 'accept',
or it may be dragged into the blacklist.
Enable Firewall
Disable Ping
Drop All
Firewall is not enabled

Figure G-21

**Step 10**. The Configuration of firewall settings is completed. See as below figure.

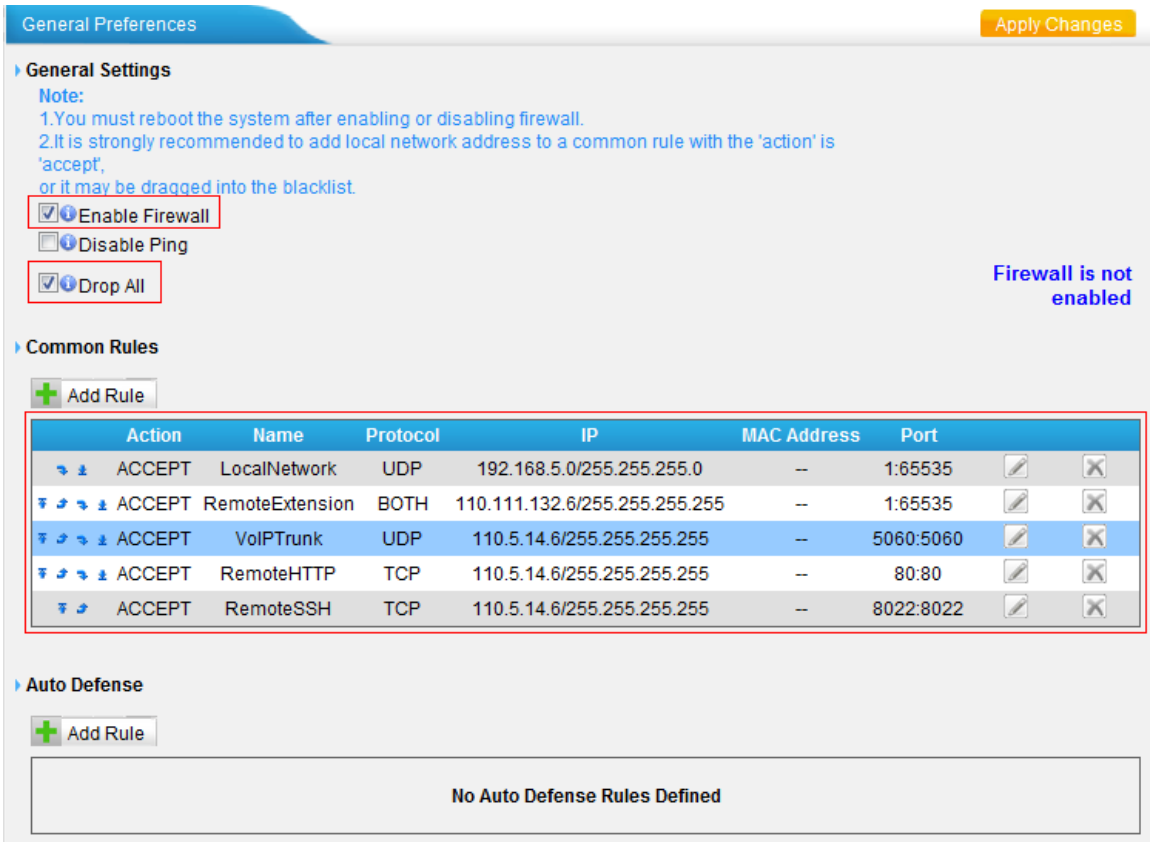

General Preferences
Apply Changes
General Settings
Note:
1.You must reboot the system after enabling or disabling firewall.
2.It is strongly recommended to add local network address to a common rule with the 'action' is 'accept',
or it may be dragged into the blacklist.
Enable Firewall
Disable Ping
Drop All
Firewall is not enabled
Common Rules
Add Rule
Action Name Protocol IP MAC Address Port
ACCEPT LocalNetwork UDP 192.168.5.0/255.255.255.0 -- 1:65535
ACCEPT RemoteExtension BOTH 110.111.132.6/255.255.255.255 -- 1:65535
ACCEPT VoIPTrunk UDP 110.5.14.6/255.255.255.255 -- 5060:5060
ACCEPT RemoteHTTP TCP 110.5.14.6/255.255.255.255 -- 80:80
ACCEPT RemoteSSH TCP 110.5.14.6/255.255.255.255 -- 8022:8022
Auto Defense
Add Rule
No Auto Defense Rules Defined

Figure G-21

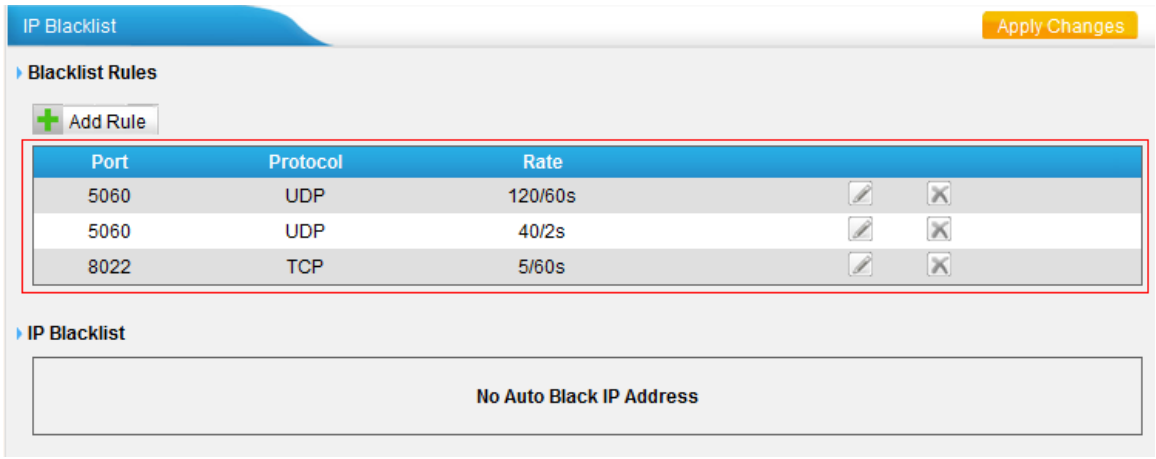



Figure G-22

**Step 11**. Define the authorized data transmitting rate and drop all other unauthorized hosts.

**Note**: If we setup IP blacklist rules here, those unauthorized hosts will still be able to send SIP packets into mPBX if the packets transmitting rate is under the rate defined. But as soon as the transmitting beyond the define rate, the IP will be added into blacklist automatically.

This is useful for remote extension who is using dynamic IP address.

Remove all the IP blacklist rules if you don't allowed any other unauthorized hosts access mPBX.See as below figure.

**Note**: If 'drop all' is not enabled, please don't remove the IP blacklist rules in case the system security hole.

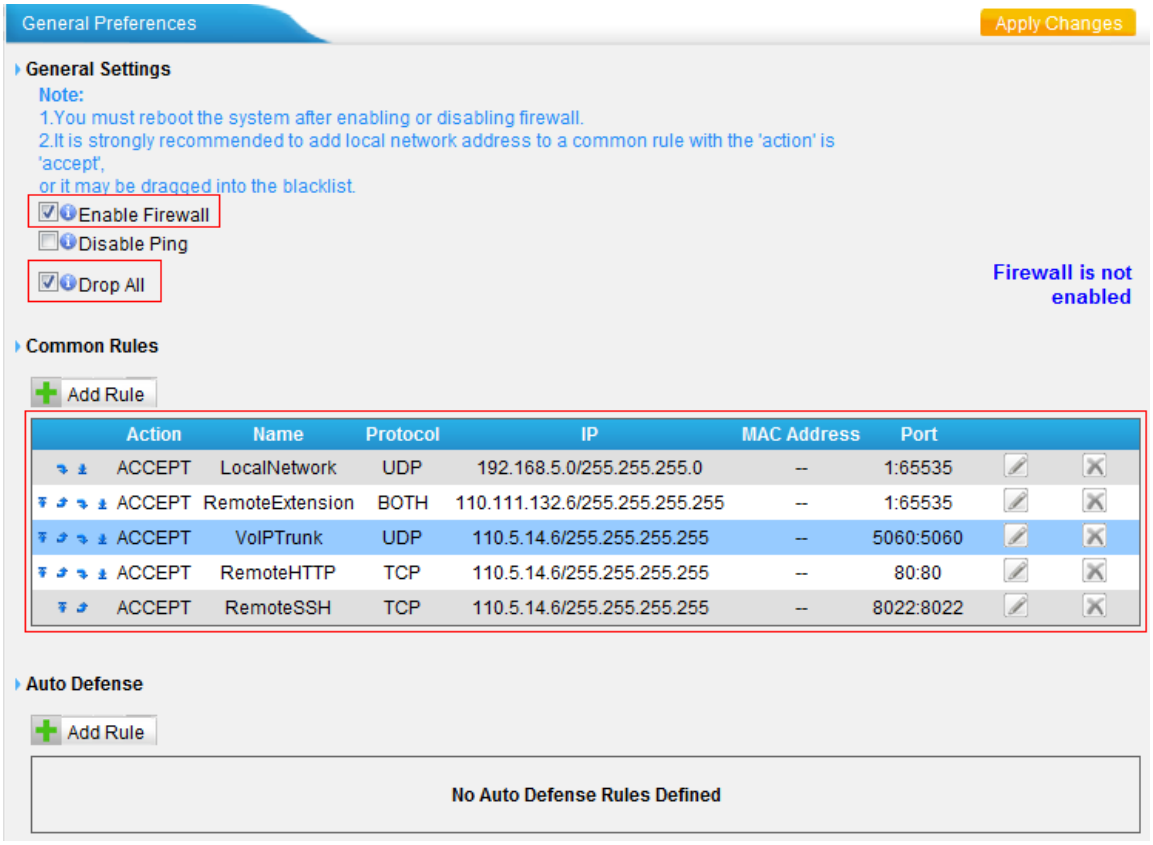

General Preferences
Apply Changes
General Settings
Note:
1.You must reboot the system after enabling or disabling firewall.
2.It is strongly recommended to add local network address to a common rule with the 'action' is 'accept',
or it may be dragged into the blacklist.
Enable Firewall
Disable Ping
Drop All
Firewall is not enabled
Common Rules
Add Rule
Action Name Protocol IP MAC Address Port
ACCEPT LocalNetwork UDP 192.168.5.0/255.255.255.0 -- 1:65535
ACCEPT RemoteExtension BOTH 110.111.132.6/255.255.255.255 -- 1:65535
ACCEPT VoIPTrunk UDP 110.5.14.6/255.255.255.255 -- 5060:5060
ACCEPT RemoteHTTP TCP 110.5.14.6/255.255.255.255 -- 80:80
ACCEPT RemoteSSH TCP 110.5.14.6/255.255.255.255 -- 8022:8022
Auto Defense
Add Rule
No Auto Defense Rules Defined

Figure G-23

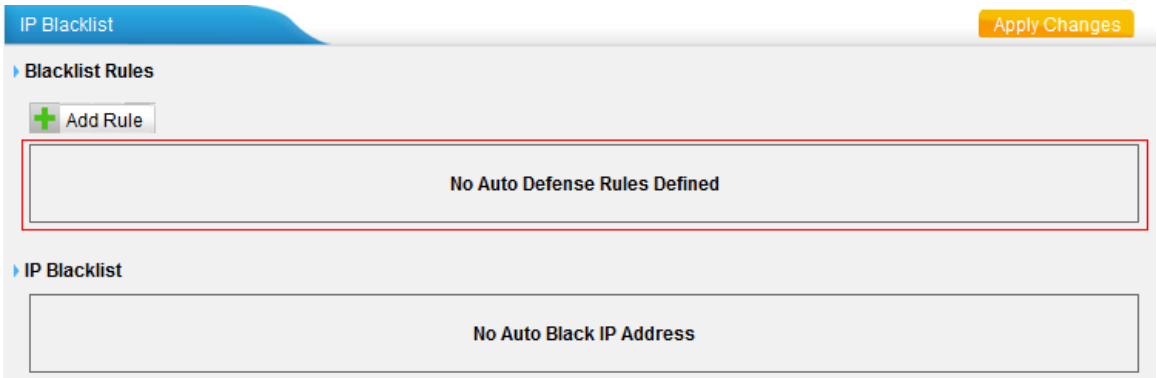



Figure G-24

# 5*. Alert Settings

After enabling alert settings', if the device is attacked, the system will notify users the alert via call or e-mail. The attack modes include IP attack and Web Login.

## 5.1 IPATTACK

When the system is attacked by some IP addresses, the firewall will add the IP to auto IP Blacklist and notify the user if it match the protection rule.
Example: Configure to notify extension 500, outbound number 5503301 and E-mail alert@yeastar.com.
configuration could be as below.
Phone Notification Settings:

**Phone Notification**: Yes
**Number**: 500;5503301
**Attempts**: 1
**Interval**: 60s
**Prompt**: default

**Note**: If there's outbound number to notify, the number should be fit with the dial pattern of outbound route.

E-mail Notification Settings:

**E-mail Notification**: Yes
**To**: alert@yeastar.com
**Subject**:IPAttack

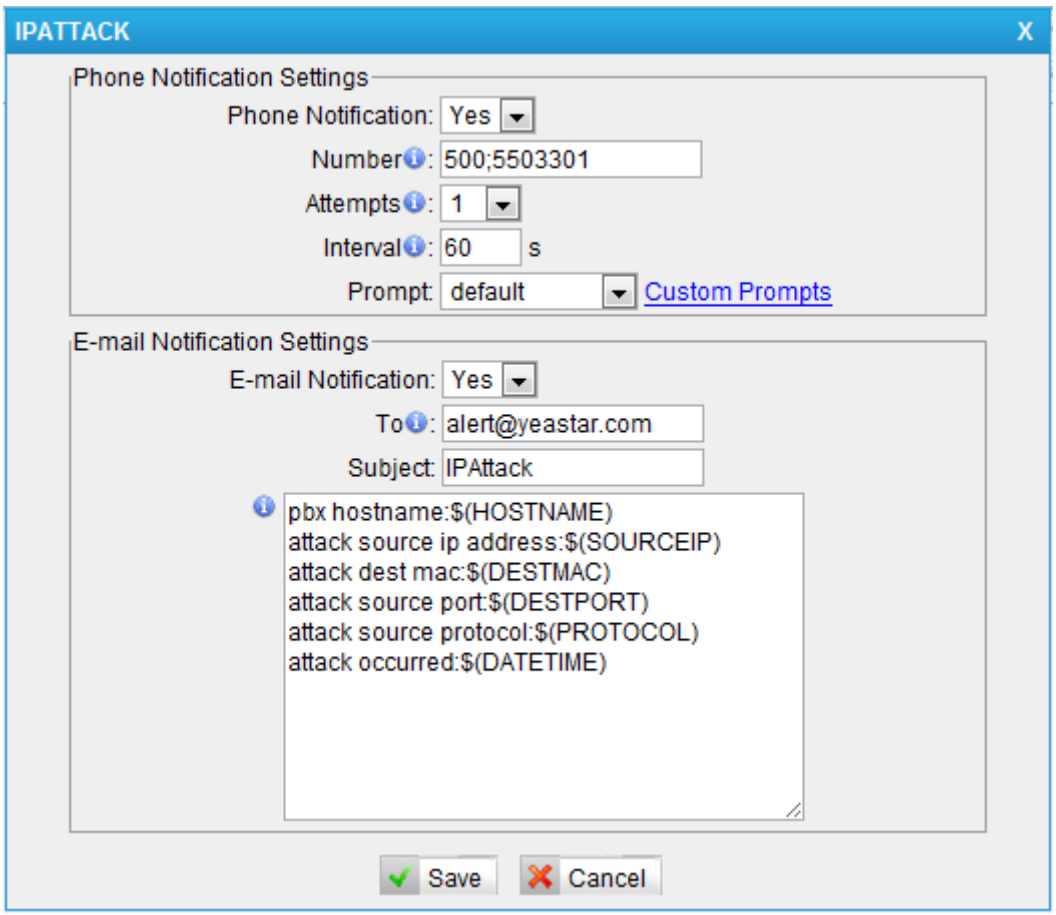



Figure G-25

## 5.2 WEBLOGIN

Enter the password incorrectly five times when logging in mPBX Web interface will be deemed as attack, the system will limit the IP login within 10 minutes and notify the user.

Example: Configure to notify extension 500, outbound number 5503301 and E-mail alert@yeastar.com.

configuration could be as below.

Phone Notification Settings:

**Phone Notification**: Yes

**Number**: 500;5503301

**Attempts**: 1

**Interval**: 60s

**Prompt**: default

**Note**: If there's outbound number to notify, the number should be fit with the dial pattern of outbound route.

E-mail Notification Settings:

**E-mail Notification**: Yes

**To**: alert@yeastar.com

**Subject**: WebLogin

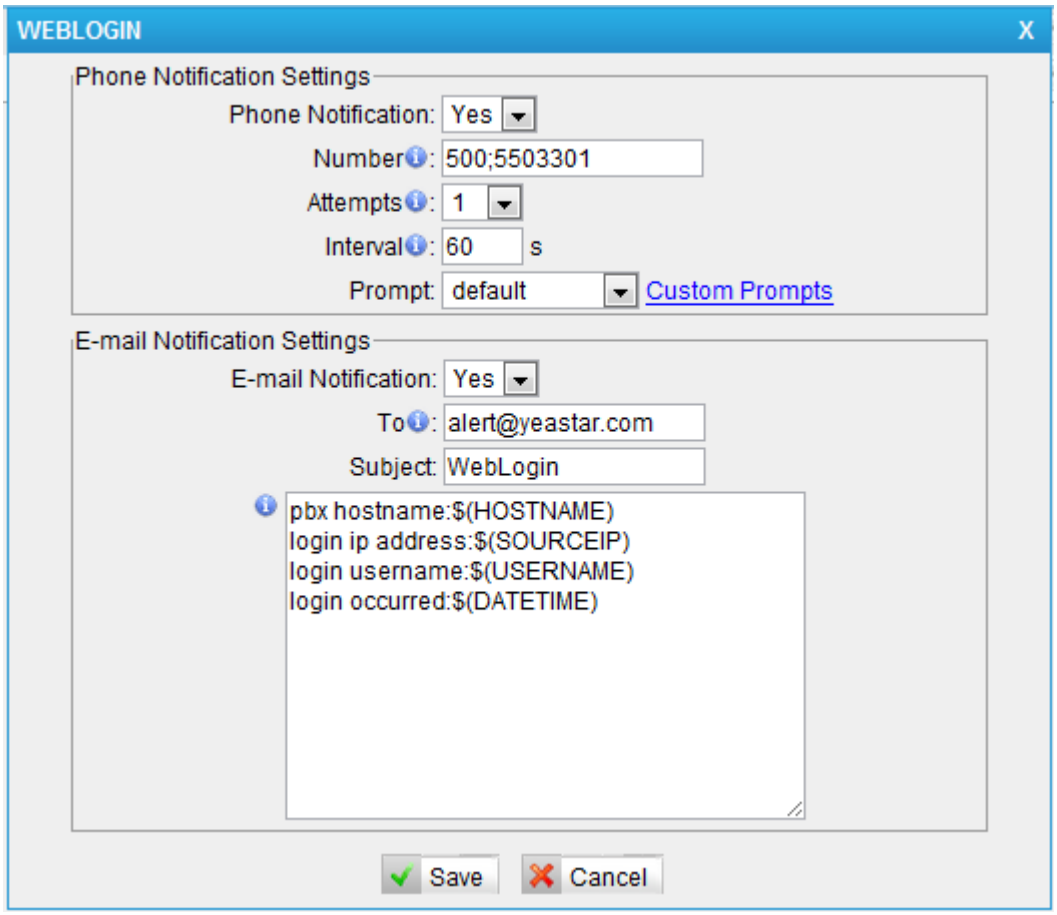



Figure G-26

# 6. Note

If the phenomena of toll fraud have been happened in your mPBX system. We are really sorry about that, then please enhance the protection level of your firewall refer to the above steps.

In addition, please change the all password: Web GUI password, SSH password, and all extensions password.

<Finish>